PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-005526
(43)Date of publication of application : 08.01.2004

(51)Int.Cl. G06F 12/14
G06F 13/00
G06F 17/60
H04L 9/08

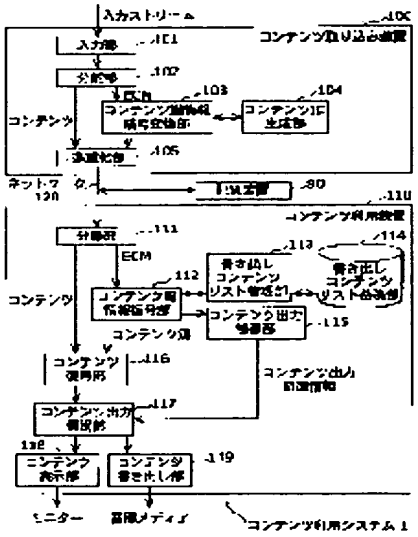
(21)Application number : 2003-092488
(22)Date of filing : 28.03.2003

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : AZUMA AKIO
TOKUDA KATSUMI
OMORI MOTOJI
INOUE MITSUHIRO

(30)Priority
Priority number : 2002103674 Priority date : 05.04.2002 Priority country : JP

(54) CONTENT USING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a content using system for satisfying mutually opposed requests such as a user request and the protection of a copyright in a well-balanced state on contents bound to a network.
SOLUTION: A content taking-in device 100 has a content ID forming part 104 for forming content ID and a content key information code converting part 103 for converting content key information into a code by a network key. A content using device 110 has a content key information decoding part 112 for decoding the content key information by the network key, a writing-out content list accumulating part 114 for accumulating a list (MCL) for recording the writing-out content ID on an accumulating medium and a writing-out content list control part 113 for determining the possibility of writing-out of the contents on the basis of the MCL.



LEGAL STATUS

[Date of request for examination] 03.02.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

THIS PAGE BLANK (USPTO)

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-5526
(P2004-5526A)
(43)公開日　平成16年1月8日(2004.1.8)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	320E	5B017
G06F 13/00	G06F 12/14	320F	5J104
G06F 17/60	G06F 13/00	540A	
H04L 9/08	G06F 17/60	142	
	H04L 9/00	601A	

審査請求 未請求　請求項の数 35　OL　（全 51 頁）　最終頁に続く

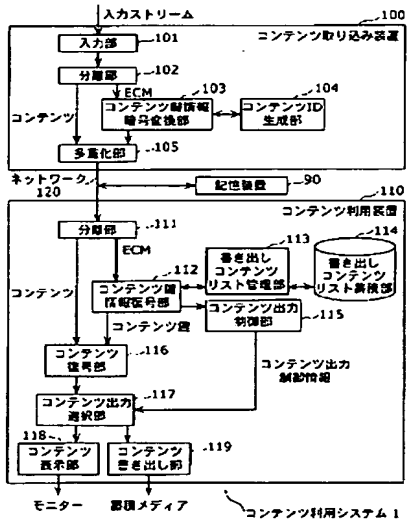
(21)出願番号　特願2003-92488 (P2003-92488)
(22)出願日　平成15年3月28日 (2003.3.28)
(31)優先権主張番号　特願2002-103674 (P2002-103674)
(32)優先日　平成14年4月5日 (2002.4.5)
(33)優先権主張国　日本国 (JP)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100109210
弁理士　新居　広守
(72)発明者　東　吾紀男
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　徳田　克己
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　大森　基司
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】コンテンツ利用システム

(57)【要約】
【課題】ネットワークにバインドされたコンテンツについて、ユーザ要求と著作権保護という相対立する要求をバランス良く解決するコンテンツ利用システムを提供する。
【解決手段】コンテンツ取り込み装置１００は、コンテンツＩＤを生成するコンテンツＩＤ生成部１０４と、ネットワーク鍵でコンテンツ鍵情報を暗号変換するコンテンツ鍵情報暗号変換部１０３とを備え、コンテンツ利用装置１１０は、コンテンツ鍵情報をネットワーク鍵で復号するコンテンツ鍵情報復号部１１２と、蓄積メディアに書き出したコンテンツのＩＤを記したリスト（ＭＣＬ）を蓄積する書き出しコンテンツリスト蓄積部１１４と、ＭＣＬに基づきコンテンツの書き出し可否判定を行う書き出しコンテンツリスト管理部１１３とを備える。
【選択図】図３



【特許請求の範囲】
【請求項１】
複数の装置が接続されたネットワークにおいてコンテンツを利用するコンテンツ利用システムであって、
前記複数の装置のうち少なくとも１つの装置に備えられ、コンテンツをネットワーク上の装置のみが利用可能な状態にすることによってコンテンツをネットワークにバインドするバインド手段と、
前記複数の装置のうち少なくとも１つの装置に備えられ、前記バインド手段によってバインドされたコンテンツに対応させてコンテンツＩＤを発行するＩＤ発行手段と、
前記複数の装置のうち少なくとも１つの装置に備えられ、前記バインド手段によってバインドされたコンテンツについて、バインドされた状態を解除するバインド解除手段と、
前記複数の装置のうち少なくとも１つの装置に備えられ、前記バインド解除手段によってバインドを解除されたコンテンツを蓄積メディアに書き出す書き出し手段と、
前記複数の装置のうち少なくとも１つの装置に備えられ、書き出し手段により書き出されたコンテンツのコンテンツＩＤを示すテーブルを記憶するテーブル手段と、
前記複数の装置のうち少なくとも１つの装置に備えられ、書き出し手段が書き出そうとするコンテンツのコンテンツＩＤを取得して、前記テーブルの内容に基づいて書き出し手段による当該コンテンツの書き出しを抑制する抑制手段と
を備えることを特徴とするコンテンツ利用システム。
【請求項２】
前記抑制手段は、書き出し手段が書き出そうとするコンテンツのコンテンツＩＤを取得し、前記テーブルに当該コンテンツＩＤが既に記録されていなければ、前記書き出し手段に対して当該コンテンツの書き出しを抑制しないで前記テーブルに取得したコンテンツＩＤを追加し、前記テーブルに当該コンテンツＩＤが既に存在していれば、前記書き出し手段に対して当該コンテンツの書き出しを抑制する
ことを特徴とする請求項１記載のコンテンツ利用システム。
【請求項３】
前記抑制手段は、書き出し手段が書き出そうとするコンテンツのコンテンツＩＤを取得して、前記テーブルに当該コンテンツＩＤが存在していなければ、当該コンテンツＩＤ及び、書き出し手段による書き出し回数を１として追加し、前記テーブルに当該コンテンツＩＤが存在し、かつ書き出し回数が予め定められた最大回数に達していれば、書き出し手段による書き出しを抑制することを特徴とする請求項１記載のコンテンツ利用システム。
【請求項４】
前記バインド手段は、前記複数の装置に共有されているネットワーク鍵を用いて、コンテンツの復号するためのコンテンツ鍵を暗号化することによって、コンテンツをネットワークにバインドする
ことを特徴とする請求項３記載のコンテンツ利用システム。
【請求項５】
前記複数の装置は、１つのコンテンツ取り込み装置と、少なくとも１つのコンテンツ利用装置とを含み、
前記コンテンツ取り込み装置は前記バインド手段と前記ＩＤ発行手段とを備え、
前記各コンテンツ利用装置は前記テーブル手段と前記バインド解除手段と前記書き出し手段と抑制手段とを備える
ことを特徴とする請求項４記載のコンテンツ利用システム。
【請求項６】
前記コンテンツ利用装置は、さらに、
書き込み手段により書き込みを行った際に少なくとも当該コンテンツＩＤを他のコンテンツ利用装置に通知する通知手段と、
他のコンテンツ利用装置から通知を受けたときに前記テーブル手段に記憶されたテーブルを更新する更新手段と

を備えることを特徴とする請求項５記載のコンテンツ利用システム。
【請求項７】
前記コンテンツ利用システムは、１つのコンテンツ取り込み装置と、少なくとも１つのコンテンツ利用装置とを含み、
前記コンテンツ取り込み装置は、前記バインド手段と、前記ＩＤ発行手段と、前記テーブル手段と、前記抑制手段とを備え、
前記各コンテンツ利用装置は、前記バインド解除手段と前記書き出し手段とを備える
ことを特徴とする請求項４記載のコンテンツ利用システム。
【請求項８】
前記コンテンツ利用システムは、１つのコンテンツ取り込み装置と、少なくとも１つのコンテンツ利用装置とを含み、
前記コンテンツ取り込み装置は、前記バインド手段と、前記ＩＤ発行手段と、前記テーブル手段とを備え、
前記各コンテンツ利用装置は、前記バインド解除手段と、前記書き出し手段と、前記抑制手段とを備える
ことを特徴とする請求項４記載のコンテンツ利用システム。
【請求項９】
前記各コンテンツ利用装置は、さらに
前記コンテンツ取り込み装置のテーブル手段に記憶された前記テーブルの内容を取得することよって、前記テーブルの写しを記憶する第２テーブル手段とを備え、
前記抑制手段は、前記テーブルの写しに基づいて抑制する
ことを特徴とする請求項８記載のコンテンツ利用システム。
【請求項１０】
前記コンテンツＩＤ発行手段は、（ａ）～（ｅ）の何れかである
（ａ）カウンタを用いて前記コンテンツＩＤを生成して発行する、（ｂ）単調増加、または、単調減少する前記コンテンツＩＤを生成して発行する、（ｃ）ユニークな値を生成する乱数を用いて前記コンテンツＩＤを生成して発行する、（ｄ）当該コンテンツと共に配信されるデータに基づいてコンテンツＩＤを生成して発行する、（ｅ）当該コンテンツと共に配信されるデータからコンテンツＩＤを取得して発行する
ことを特徴とする請求項４に記載のコンテンツ利用システム。
【請求項１１】
前記コンテンツＩＤ発行手段は、さらに、
前記コンテンツ取り込み装置を識別するためのＩＤを関連づけて前記コンテンツＩＤ生成する
ことを特徴とする請求項４項に記載のコンテンツ利用システム。
【請求項１２】
前記コンテンツＩＤ発行手段は、
前記コンテンツＩＤを、放送番組に対応するコンテンツ毎に生成する
ことを特徴とする請求項４に記載のコンテンツ利用システム。
【請求項１３】
前記テーブルは、コンテンツＩＤ毎にコンテンツの書き出し先を示す情報を含み、
前記抑制手段は、前記情報が示す書き出し先と、書き出し手段が書き出そうとする書き出し先とが異なる場合は、書き出しを抑制する
ことを特徴とする請求項４記載のコンテンツ利用システム。
【請求項１４】
前記テーブルは、コンテンツＩＤ毎にコンテンツの書き出し形態を示す情報を含み、
前記抑制手段は、前記情報が示す書き出し形態と、書き出し手段が書き出そうとする書き出し形態とが異なる場合は、書き出しを抑制する
ことを特徴とする請求項４記載のコンテンツ利用システム。
【請求項１５】

前記テーブルは、コンテンツの単位時間あたりの書き出し可能回数の情報を含み、
前記抑制手段は、書き出し手段による単位時間あたりコンテンツ書き出し回数が、単位時間あたりの書き出し可能回数を超えている場合は、書き出しを抑制する
ことを特徴とする請求項４記載のコンテンツ利用システム。
【請求項１６】
前記テーブルは、コンテンツの書き出し完了から、次にコンテンツを書き出し開始可能となる迄の時間間隔の情報を含み、
前記抑制手段は、書き出し手段によるコンテンツ書き出しの時間間隔が、前記時間間隔より短い場合は、書き出しを抑制する
ことを特徴とする請求項４記載のコンテンツ利用システム。
【請求項１７】
前記テーブルのハッシュ値を、前記テーブル手段でセキュアに管理する
ことを特徴とする請求項４記載のコンテンツ利用システム。
【請求項１８】
前記テーブル手段は、前記テーブルに記録されたコンテンツＩＤを削除するためのしきい値を記憶し、前記テーブルに記録されたコンテンツＩＤの数が前記しきい値に達したとき、前記テーブルから少なくとも１つのコンテンツＩＤを削除する
ことを特徴とする請求項４記載のコンテンツ利用システム。
【請求項１９】
前記テーブルは、さらに、コンテンツＩＤを登録した日時を示す日時情報を記録し、
前記テーブル手段は、前記テーブルに記録されたコンテンツＩＤの数が前記しきい値に達したとき、前記日時情報に基づいて削除すべきコンテンツＩＤを決定する
ことを特徴とする請求項１８に記載のコンテンツ利用システム。
【請求項２０】
前記テーブルは、さらに、該当コンテンツへのアクセス情報を記録し、
前記テーブル手段は、前記テーブルに記録されたコンテンツＩＤの数が前記しきい値に達したとき、前記アクセス情報に基づいて削除すべきコンテンツＩＤを決定する
ことを特徴とする請求項１８に記載のコンテンツ利用システム。
【請求項２１】
前記テーブル手段は、前記テーブルに記録されたコンテンツＩＤ数が前記しきい値に達したとき、乱数を生成して当該乱数に基づいて削除すべきコンテンツＩＤを決定する
ことを特徴とする請求項１８に記載のコンテンツ利用システム。
【請求項２２】
ネットワーク鍵を共有するコンテンツ取り込み装置と１以上のコンテンツ利用装置とを含み、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ利用システムであって、
前記コンテンツ取り込み装置は、
コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、
取得手段により取得されたコンテンツを識別するためのコンテンツＩＤを生成するＩＤ生成手段と、
取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情報にコンテンツＩＤを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と、
を備え、
前記各コンテンツ利用装置は、
ネットワーク鍵を用いて暗号化されたコンテンツ鍵情報を復号する第１復号手段と、
第１復号手段により復号されたコンテンツ鍵情報中のコンテンツ鍵を用いて前記コンテンツを復号する第２復号手段と、

第２復号手段によって復号されたコンテンツを蓄積メディアに書き出す書き出し手段と、
第１復号手段により復号されたコンテンツ鍵情報に含まれるコンテンツＩＤと、当該コンテンツＩＤに対応するコンテンツが前記書き出し手段によって書き出された回数とを対応させたテーブルを記憶するテーブル記憶手段と、
前記書き出し手段が書き出そうとするコンテンツのコンテンツＩＤを取得して、前記テーブルから当該コンテンツＩＤに対応するコンテンツが書き出された回数を参照し、当該回数が予め定められた最大回数に達していれば、書き出し手段による当該コンテンツの書き出しを抑制する抑制手段と
を備える
ことを特徴とするコンテンツ利用システム。

【請求項２３】
前記コンテンツ利用装置は、さらに、第２復号手段によって復号されたコンテンツを再生する再生手段を有し、
前記抑制手段は、さらに、前記再生手段が再生しようとするコンテンツのコンテンツＩＤを取得して、前記テーブルから当該コンテンツＩＤに対応するコンテンツが書き出された回数を参照し、当該回数が前記最大回数に達していれば、再生手段による再生を抑制することを特徴とする請求項２２記載のコンテンツ利用システム。

【請求項２４】
前記コンテンツ利用装置は、さらに、
前記テーブルを、他のコンテンツ利用装置のテーブルと同期するためのテーブル同期手段を備え、
前記テーブル同期手段は、前記テーブルが更新されたとき、前記他のコンテンツ利用装置におけるテーブル同期手段に対し、少なくとも前記コンテンツＩＤを含む同期情報を送信し、前記他のコンテンツ利用装置におけるテーブル同期手段から同期情報を受信したとき、前記テーブル記憶手段の前記テーブルを更新する
ことを特徴とする請求項２２記載のコンテンツ利用システム。

【請求項２５】
ネットワーク鍵を共有するコンテンツ取り込み装置と１つ以上のコンテンツ利用装置とを含み、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ利用システムであって、
前記各コンテンツ取り込み装置は、
コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、
取得されたコンテンツを識別するためのコンテンツＩＤを生成するＩＤ生成手段と、
取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情報にコンテンツＩＤを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と、
前記コンテンツ利用装置において蓄積メディアに書き出したコンテンツのコンテンツＩＤを記録するためのテーブルを記憶するテーブル記憶手段と、
前記コンテンツ利用装置から書き出し可否判定要求を受けたとき、前記テーブルを用いてコンテンツの書き出し可否判定を行い、書き出し可否判定結果に基づいて前記テーブルを更新するテーブル管理手段と、
前記コンテンツ利用装置から書き出し可否判定要求を受信し、前記テーブル管理手段から取得した書き出し可否判定結果を送信するコンテンツＩＤ受信手段と、
を備え、
前記コンテンツ利用装置は、
再暗号化されたコンテンツ鍵情報を前記ネットワーク鍵を用いて復号する第１復号手段と、
前記コンテンツ取り込み装置に対し、復号されたコンテンツ鍵情報に含まれるコンテンツ

ＩＤを含む書き出し可否判定要求を送信し、書き出し可否判定結果を受信するコンテンツＩＤ送信手段と、
受信された書き出し可否判定結果が可を示す場合のみ、第１復号手段により復号されたコンテンツ鍵情報に含まれるコンテンツ鍵を用いてコンテンツを復号する第２復号手段と、
第２復号手段により復号されたコンテンツを蓄積メディアに書き出す書き出し手段と、
を備えることを特徴とするコンテンツ利用システム。
【請求項２６】
ネットワーク鍵を共有するコンテンツ取り込み装置と１つ以上のコンテンツ利用装置とを含み、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ利用システムであって、
前記コンテンツ取り込み装置は、
コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、
取得されたコンテンツを識別するためのコンテンツＩＤを生成するＩＤ生成手段と、
取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情報にコンテンツＩＤを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と、
前記コンテンツ利用装置において蓄積メディアに書き出したコンテンツのコンテンツＩＤを記録するためのテーブルを記憶する第１テーブル記憶手段と、
前記コンテンツ利用装置から書き出し可否判定要求を受けたとき、前記テーブルを用いてコンテンツの書き出し可否判定を行い、書き出し可否判定結果に基づいて前記テーブルを更新するテーブル管理手段と、
前記コンテンツ利用装置から前記同期情報を受信し、前記テーブルを前記コンテンツ利用装置に送信するテーブル送信手段と、
を備え、
前記コンテンツ利用装置は、
再暗号化された前記コンテンツ鍵情報を前記ネットワーク上で予め共有されている暗号鍵を用いて復号し、前記コンテンツ鍵を出力する第１復号手段と、
前記コンテンツ取り込み装置に対し、少なくともコンテンツＩＤを含む前記テーブルの同期情報を送信し、前記テーブルを受信するテーブル受信手段と、
前記テーブルを記憶する第２テーブル記憶手段と、
前記コンテンツ取り込み装置から受信した前記テーブルで、前記第２テーブル記憶手段のテーブルを更新し、前記テーブルを用いてコンテンツの書き出し可否判定を行うテーブル管理手段と、
テーブル管理手段による判定結果が可を示す場合のみ、暗号化された前記コンテンツを前記コンテンツ鍵で復号する第２復号手段と、
第２復号手段により復号されたコンテンツを蓄積メディアに書き出す書き出し手段と
を備えることを特徴とするコンテンツ利用システム。
【請求項２７】
ネットワーク鍵を共有するコンテンツ取り込み装置と１つ以上のコンテンツ利用装置と前記コンテンツ利用装置に接続され蓄積メディアにコンテンツを書き出すコンテンツ書き出し装置とを含み、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ利用システムであって、
前記コンテンツ取り込み装置は、
コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、
取得されたコンテンツを識別するためのコンテンツＩＤを生成するＩＤ生成手段と、
取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情

報にコンテンツＩＤを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と
を備え、
前記コンテンツ利用装置は、
ネットワーク鍵を用いて再暗号化されたコンテンツ鍵情報を復号する第１復号手段と、
復号されたコンテンツ鍵情報に含まれるコンテンツ鍵で前記コンテンツを復号する第２復号手段と
を備え、
前記コンテンツ書き出し部は、
蓄積メディアにコンテンツを書き出す書き出し手段と、
コンテンツ書き出し手段から蓄積メディアに書き出したコンテンツのコンテンツＩＤを記録するための、テーブルを記憶するテーブル記憶手段と、
前記テーブルを用いてコンテンツの書き出し可否判定を行い、判定結果に従って書き出し手段を制御するテーブル管理手段と
を備えることを特徴とするコンテンツ利用システム。
【請求項２８】
前記第１復号手段は、任意の単位で単調増加または単調減少するＩＤを生成して、前記ＩＤを前記第２復号手段に送信し、
前記第２復号手段は、受信した前記ＩＤを記録し、書き出し処理を再開する場合に、前記ＩＤを前記第１復号手段に送信し、
前記第１復号手段は、受信した前記ＩＤと最後に生成した前記ＩＤとを比較して、差分がある値以下である場合にのみ、書き出し処理の再開を許可する
ことを特徴とする請求項２２記載のコンテンツ利用システム。
【請求項２９】
コンテンツ取り込み装置と、１以上の前記コンテンツ利用装置とがネットワーク接続されるコンテンツ利用システムであって、
前記コンテンツ取り込み装置は、
暗号化された前記コンテンツ鍵情報を復号し、前記コンテンツ鍵に作用させるための秘密情報を生成し、前記ネットワークで予め共有された暗号鍵と、前記秘密情報とを用いて前記コンテンツ鍵情報を再暗号化する暗号変換手段と、
前記コンテンツ利用装置から、コンテンツの出力要求を受信し、少なくとも前記秘密情報を含む要求応答を送信する出力要求処理手段と、
を備え、
前記コンテンツ利用装置は、
前記コンテンツ取り込み装置に対し、少なくともコンテンツの出力先を含む出力要求を送信し、要求応答を受信して前記秘密情報を取得する出力要求手段と、
前記ネットワークで予め共有された暗号鍵と、前記秘密情報とを用いて、再暗号化された前記コンテンツ鍵情報を復号する第１復号手段と、
選択手段を制御するためのコンテンツ出力制御情報を出力する制御手段と、
暗号化された前記コンテンツを前記コンテンツ鍵で復号する第２復号手段と、
前記コンテンツ出力制御情報に基づき、前記コンテンツの出力先を選択する選択手段と、
前記コンテンツを出力するための１以上の出力手段と
を備えることを特徴とするコンテンツ利用システム。
【請求項３０】
コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによってネットワークにバインドされたコンテンツを利用するコンテンツ利用装置であって、
ネットワーク鍵を用いて再暗号化されたコンテンツ鍵情報を復号する第１復号手段と、
第１復号手段により復号されたコンテンツ鍵情報中のコンテンツ鍵を用いて前記コンテンツを復号する第２復号手段と、

第２復号手段によって復号されたコンテンツを蓄積メディアに書き出す書き出し手段と、
第１復号手段により復号されたコンテンツ鍵情報に含まれるコンテンツＩＤと、当該コンテンツＩＤに対応するコンテンツが前記書き出し手段によって書き出された回数とを対応させたテーブルを記憶するテーブル記憶手段と、
前記書き出し手段が書き出そうとするコンテンツのコンテンツＩＤを取得して、前記テーブルから当該コンテンツＩＤに対応するコンテンツが書き出された回数を参照し、当該回数が予め定められた最大回数に達していれば、書き出し手段による当該コンテンツの書き出しを抑制する抑制手段と
を備えることを特徴とするコンテンツ利用装置。
【請求項３１】
ネットワーク鍵を共有する複数の装置が接続されてネットワークにおいて、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ取り込み装置であって、
コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、
取得手段により取得されたコンテンツを識別するためのコンテンツＩＤを生成するＩＤ生成手段と、
取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情報にコンテンツＩＤを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と、
を備え、
前記コンテンツＩＤは、ネットワークにバインドされたコンテンツを、バインドされていない状態で蓄積メディアに書き出すことを管理するために用いられることを特徴とするコンテンツ取り込み装置。
【請求項３２】
複数の装置が接続されたネットワークにおいてコンテンツを利用するコンテンツ利用方法であって、
前記複数の装置のうち少なくとも１つの装置において、コンテンツをネットワーク上の装置のみが利用可能な状態にすることによってコンテンツをネットワークにバインドするバインドステップと、
前記複数の装置のうち少なくとも１つの装置において、前記バインドステップにおいてバインドされたコンテンツに対応させてコンテンツＩＤを発行するＩＤ発行ステップと、
前記複数の装置のうち少なくとも１つの装置において、ネットワークにバインドされたコンテンツをバインドされていない状態にしてこれから書き出そうとするコンテンツのコンテンツＩＤを取得して、既に書き出されたコンテンツのＩＤを記録したテーブルをメモリから参照して、書き出し可否を判定する判定ステップと、
前記複数の装置のうち少なくとも１つの装置において、判定ステップにおいて書き出し可と判定された場合に、前記バインドステップにおいてバインドされたコンテンツについて、バインドされた状態を解除するバインド解除ステップと、
前記複数の装置のうち少なくとも１つの装置において、バインド解除ステップにおいてバインドを解除されたコンテンツを蓄積メディアに書き出す書き出しステップと、
を有することを特徴とするコンテンツ利用方法。
【請求項３３】
コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによってネットワークにバインドされたコンテンツを利用する装置におけるコンテンツ利用方法であって、
ネットワーク鍵を用いて再暗号化されたコンテンツ鍵情報を復号する第１復号ステップと、
第１復号ステップにおいて復号されたコンテンツ鍵情報中のコンテンツ鍵を用いて前記コ

ンテンツを復号する第２復号ステップと、
ネットワークにバインドされたコンテンツをバインドされていない状態にしてこれから書き出そうとするコンテンツのコンテンツＩＤを取得して、既に書き出されたコンテンツのＩＤを記録したテーブルをメモリから参照して、書き出し可否を判定する判定ステップと、
判定ステップにおいて書き出し可と判定された場合に、前記バインドされたコンテンツについて、バインドされた状態を解除してバインドされていない状態で蓄積メディアに書き出す書き出しステップと、
を有することを特徴とするコンテンツ利用方法。
【請求項３４】
ネットワーク鍵を共有するコンテンツ取り込み装置と１以上のコンテンツ利用装置とを含み、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ利用システムにおいて、コンテンツ取り込み装置において実行される第１プログラムと、コンテンツ利用装置において実行される第２プログラムとからなるコンテンツ利用プログラムであって、
前記第１プログラムは、
コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、
取得手段により取得されたコンテンツを識別するためのコンテンツＩＤを生成するＩＤ生成手段と、
取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情報にコンテンツＩＤを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と
を含む各手段をコンピュータに機能させ、
前記第２プログラムは、
ネットワーク鍵を用いて再暗号化されたコンテンツ鍵情報を復号する第１復号手段と、
第１復号手段により復号されたコンテンツ鍵情報中のコンテンツ鍵を用いて前記コンテンツを復号する第２復号手段と、
第２復号手段によって復号されたコンテンツを蓄積メディアに書き出す書き出し手段と、
第１復号手段により復号されたコンテンツ鍵情報に含まれるコンテンツＩＤと、当該コンテンツＩＤに対応するコンテンツが前記書き出し手段によって書き出された回数とを対応させたテーブルを記憶するテーブル記憶手段と、
前記書き出し手段が書き出そうとするコンテンツのコンテンツＩＤを取得して、前記テーブルから当該コンテンツＩＤに対応するコンテンツが書き出された回数を参照し、当該回数が予め定められた最大回数に達していれば、書き出し手段による当該コンテンツの書き出しを抑制する抑制手段と
を含む各手段をコンピュータに機能させる
ことを特徴とするコンテンツ利用プログラム。
【請求項３５】
コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによってネットワークにバインドされたコンテンツを利用する装置において実行されるコンテンツ利用プログラムであって、
前記プログラムは、
ネットワーク鍵を用いて再暗号化されたコンテンツ鍵情報を復号する第１復号手段と、
第１復号手段により復号されたコンテンツ鍵情報中のコンテンツ鍵を用いて前記コンテンツを復号する第２復号手段と、
第２復号手段によって復号されたコンテンツを蓄積メディアに書き出す書き出し手段と、
第１復号手段により復号されたコンテンツ鍵情報に含まれるコンテンツＩＤと、当該コンテンツＩＤに対応するコンテンツが前記書き出し手段によって書き出された回数とを対応

させたテーブルを記憶するテーブル記憶手段と、
前記書き出し手段が書き出そうとするコンテンツのコンテンツＩＤを取得して、前記テーブルから当該コンテンツＩＤに対応するコンテンツが書き出された回数を参照し、当該回数が予め定められた最大回数に達していれば、書き出し手段による当該コンテンツの書き出しを抑制する抑制手段と
を含む各手段をコンピュータに機能させる
ことを特徴とするコンテンツ利用プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、通信や放送などで配信された映像や音声などのデジタルコンテンツを利用するシステムに関し、特に、コンテンツを外部蓄積メディアに書き出す場合のコンテンツの利用制御に関する。
【０００２】
【従来の技術】
近年、音楽や映像、ゲームなどのデジタルコンテンツをインターネットやデジタル放送で配信し、利用するシステムが実用化の段階を迎えている。
【０００３】
従来のコンテンツ利用システムでは、特許文献１～３に見られるように、放送で配信されたコンテンツをネットワークにバインドすることにより、コンテンツをネットワーク内で共有し、利用することができる。ここで、コンテンツをネットワークにバインドするというのは、ネットワーク内の正当な端末のみが当該コンテンツを利用できる状態にすることをいう。言い換えれば、正当でない他の端末がネットワークに接続されても、当該他の端末が当該コンテンツを利用できない状態にすることをいう。あるいは、ネットワークにバインドされたコンテンツを他のネットワークに移動させた場合も、他のネットワークの端末が当該コンテンツを利用できない状態にすることをいう。
【０００４】
例えば、暗号化されて配信されたコンテンツをネットワーク（例えば、家庭内ネットワーク）に取り込む場合、暗号化されたコンテンツは変換せずそのままネットワーク内の端末が利用し、コンテンツの暗号鍵を暗号変換することによって、コンテンツをネットワークにバインドすることができる。ここで暗号変換は、暗号鍵を一旦復号した上で、さらにネットワーク上で予め共有されている暗号鍵（以下、ネットワーク鍵と記す）を用いて、コンテンツの暗号鍵を再暗号化することをいう。
【０００５】
ネットワークにバインドされたコンテンツを利用する場合、ネットワーク鍵を保持しているネットワーク上の機器は、共有しているネットワーク鍵を用いてコンテンツの再暗号化された暗号鍵を復号することができるので、復号された暗号鍵を用いて暗号化されたコンテンツを復号することができる。
【０００６】
一方、ネットワーク鍵を保持していない機器は、コンテンツの暗号鍵を復号することができないため、暗号化されたコンテンツも復号することができないようになっている。
【０００７】
下記特許文献１～３等の従来のコンテンツ利用システムでは、ネットワークにコンテンツをバインドすると、ハードディスク等のネットワーク上の蓄積媒体にコンテンツとコンテンツ暗号鍵のコピーをネットワークにバインドされた状態で作成することが無制限に可能であるが、その利用（再生等）に関しては、ネットワーク機器の数を制限することによって、制限を課するようになっている。
【０００８】
【特許文献１】
特開平１１－３３１８０５号公報

【０００９】
【特許文献２】
米国特許公報５８７８１３５号明細書
【００１０】
【特許文献３】
米国特許公報６０１６３４８号明細書
【００１１】
【発明が解決しようとする課題】
ところで、上記従来技術によれば、ネットワークにバインドされていない状態でコンテンツをネットワーク外に書き出すことが実際上できないようになっている。これに対して、ネットワークにバインドされたコンテンツをＤＶＤ－ＲＡＭ、Ｄ－ＶＨＳ、ＳＤカード等のメモリカードといった外部蓄積メディアに書き出して（ＭＯＶＥ、ＥＸＰＯＲＴ等）コンテンツを利用したいといったユーザの要求がある。
【００１２】
このように、従来のコンテンツ利用システムでは、バインドされていない状態で書き出すことは考慮されておらず、上記のようなユーザの要求を満たすことができないという問題がある。
【００１３】
また、仮に、コンテンツをバインドしていない状態で書き出すことが可能であると仮定しても、蓄積メディアへのコンテンツのコピーが無制限に作成できてしまう恐れがあり、コンテンツの著作権保護の観点から問題が生ずることになる。
【００１４】
本発明は、こうした従来の問題点に鑑み、ネットワークにバインドされたコンテンツについて、上記のユーザ要求と著作権保護という相対立する要求をバランス良く解決するコンテンツ利用システムを提供することを目的とする。
【００１５】
言い換えれば、ネットワークにバインドされたコンテンツを蓄積メディアに書き出したいというユーザ要求を満たしながら十分な著作権保護を可能にするコンテンツ利用システムを提供することを目的とする。
【００１６】
【課題を解決するための手段】
上記目的を達成するために、本発明におけるコンテンツ利用システムは、複数の装置が接続されたネットワークにおいてコンテンツを利用するコンテンツ利用システムであって、前記複数の装置のうち少なくとも１つの装置に備えられ、コンテンツをネットワーク上の装置のみが利用可能な状態にすることによってコンテンツをネットワークにバインドするバインド手段と、前記複数の装置のうち少なくとも１つの装置に備えられ、前記バインド手段によってバインドされたコンテンツに対応させてコンテンツＩＤを発行するＩＤ発行手段と、前記複数の装置のうち少なくとも１つの装置に備えられ、前記バインド手段によってバインドされたコンテンツについて、バインドされた状態を解除するバインド解除手段と、前記複数の装置のうち少なくとも１つの装置に備えられ、前記バインド解除手段によってバインドを解除されたコンテンツを蓄積メディアに書き出す書き出し手段と、前記複数の装置のうち少なくとも１つの装置に備えられ、書き出し手段により書き出されたコンテンツのコンテンツＩＤを示すテーブルを記憶するテーブル手段と、前記複数の装置のうち少なくとも１つの装置に備えられ、書き出し手段が書き出そうとするコンテンツのコンテンツＩＤを取得して、前記テーブルの内容に基づいて書き出し手段による当該コンテンツの書き出しを抑制する抑制手段とを備える。
【００１７】
この構成によれば、ネットワークにバインドされたコンテンツ毎に、コンテンツＩＤを付与して、コンテンツの書き出しテーブルによって管理するので、書き出し手段によって無制限に書き出しすることを抑制することができる。つまり、ネットワークにバインドされ

ていない状態で書き出すことを制限することができる。例えば、家庭内のネットワークにバインドされたコンテンツを蓄積メディアに書き出したいという個人ユーザの要求を満たしながらも著作権を十分に保護することができるので、ユーザの私的利用と著作権者との間の相対立する利益をバランスよく満たすことができる。

【００１８】

ここで、前記抑制手段は、書き出し手段が書き出そうとするコンテンツのコンテンツＩＤを取得し、前記テーブルに当該コンテンツＩＤが既に記録されていなければ、前記書き出し手段に対して当該コンテンツの書き出しを抑制しないで前記テーブルに取得したコンテンツＩＤを追加し、前記テーブルに当該コンテンツＩＤが既に存在していれば、前記書き出し手段に対して当該コンテンツの書き出しを抑制する構成としてもよい。

【００１９】

この構成によれば、抑制手段は前記テーブルに当該コンテンツＩＤが既に存在していれば、前記書き出し手段に対して当該コンテンツの書き出しを抑制するので、書き出し手段による書き出しをコンテンツ毎に１回許可し、２回目以降を禁止することができる。

【００２０】

ここで、前記抑制手段は、書き出し手段が書き出そうとするコンテンツのコンテンツＩＤを取得して、前記テーブルに当該コンテンツＩＤが存在していなければ、当該コンテンツＩＤ及び、書き出し手段による書き出し回数を１として追加し、前記テーブルに当該コンテンツＩＤが存在し、かつ書き出し回数が予め定められた最大回数に達していれば、書き出し手段による書き出しを抑制する構成としてもよい。

【００２１】

この構成によれば、抑制手段は、前記テーブルに当該コンテンツＩＤが存在し、かつ書き出し回数が予め定められた最大回数に達していれば、書き出し手段による書き出しを抑制するので、書き出し手段による書き出しをコンテンツ毎に最大回数の範囲内で許可し、それを超える場合は禁止することができる。最大回数は１つの値を予め定めておいてもよいし、コンテンツ毎に予め定めておいてもよいので、ユーザと著作権者との相対立する利益をより柔軟にバランスをとることができる。

【００２２】

ここで、前記バインド手段は、前記複数の装置に共有されているネットワーク鍵を用いて、コンテンツの復号するためのコンテンツ鍵を暗号化することによって、コンテンツをネットワークにバインドする構成としてもよい。

【００２３】

この構成によれば、コンテンツそのものをネットワーク鍵で暗号化する必要はないので、バインドするための処理負荷を小さくすることができる。

ここで、前記複数の装置は、１つのコンテンツ取り込み装置と、少なくとも１つのコンテンツ利用装置とを含み、前記コンテンツ取り込み装置は前記バインド手段と前記ＩＤ発行手段とを備え、前記各コンテンツ利用装置は前記テーブル手段と前記バインド解除手段と前記書き出し手段と抑制手段とを備える構成としてもよい。

【００２４】

この構成によれば、コンテンツのバインド及びコンテンツＩＤの生成は、ネットワーク上に１つ存在するコンテンツ取り込み装置において集中して処理することができる。

【００２５】

ここで、前記コンテンツ利用装置は、さらに、書き込み手段により書き込みを行った際に少なくとも当該コンテンツＩＤを他のコンテンツ利用装置に通知する通知手段と、他のコンテンツ利用装置から通知を受けたときに前記テーブル手段に記憶されたテーブルを更新する更新手段とを備える構成としてもよい。

【００２６】

この構成によれば、ネットワーク上の複数のコンテンツ利用装置の間でとテーブルの内容を容易に一致させることができる。

ここで、前記コンテンツ利用システムは、１つのコンテンツ取り込み装置と、少なくとも

１つのコンテンツ利用装置とを含み、前記コンテンツ取り込み装置は、前記バインド手段と、前記ＩＤ発行手段と、前記テーブル手段と、前記抑制手段とを備え、前記各コンテンツ利用装置は、前記バインド解除手段と前記書き出し手段とを備える構成としてもよい。

【００２７】

この構成によれば、コンテンツのバインドと、コンテンツＩＤの生成と、テーブルの管理と、書き出しの抑制とを、ネットワーク上に１つ存在するコンテンツ取り込み装置において集中して処理することができる。各コンテンツ利用手段は、コンテンツ取り込み装置における抑制手段に従って書き出しを行えばよいので、テーブルを個別に管理する負荷がかからない。

【００２８】

また、本発明のコンテンツ利用方法及びコンテンツ利用プログラムについても上記と同様の構成、作用及び効果を有する。

【００２９】

【発明の実施の形態】

（実施の形態１）

以下、本発明の実施の形態１について、図面を用いて詳細に説明する。

【００３０】

図１は、本発明の実施の形態１に関わるコンテンツ利用システム１の全体の構成を示す図である。

このコンテンツ利用システムは、デジタル放送で配信されるコンテンツを、ネットワークで接続された機器で利用するシステムであり、コンテンツを取り込むためのコンテンツ取り込み装置１００と、記憶装置９０と、コンテンツを利用する複数のコンテンツ利用装置１１０－１、１１０－２、１１０－３等と、これらを接続するネットワーク１２０とから構成される。

【００３１】

コンテンツ取り込み装置１００は、放送波からコンテンツを取り込み、少なくともコンテンツの暗号鍵（以下、コンテンツ鍵と記す）を含む、暗号化されたコンテンツ鍵情報を復号し、ネットワークで予め共有された暗号鍵（以下、ネットワーク鍵と記す）を用いてコンテンツ鍵情報を再暗号化、すなわち暗号変換することにより、コンテンツをネットワークにバインドする。

【００３２】

例えば、コンテンツ取り込み装置１００は、図２に示すように、デジタル放送を受信するためのＳＴＢ（Ｓｅｔ　ＴｏＰ　Ｂｏｘ）であり、ＣＡＳ（Ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ　Ｓｙｓｔｅｍ）でアクセス制御されたコンテンツと、アクセス鍵情報としてコンテンツ鍵を含む暗号化されたＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ）とを受信し、ＥＣＭセクションを再構成して、暗号化されたＥＣＭの暗号を一旦復号し、ネットワーク鍵で再暗号化して、ネットワーク１２０にコンテンツと再暗号化したＥＣＭを流す、といった処理を行う。なお、ＥＣＭは、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓで規定されたＰｒｉｖａｔｅセクションで実現され、図４で示されるような構造となっている。なお、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓは、国際標準であるＩＳＯ／ＩＥＣ１３８１８－１に規定されている。

【００３３】

図４に示したＥＣＭセクションは、セクションヘッダとＥＣＭ本体とセクションテーラ（誤り検出符号）を有する構造となっている。同図のＥＣＭセクションには、ＥＣＭ本体の内容の一例として、バージョン番号、コピー制御情報、コンテンツ鍵、可変長のプライベートデータ、改ざん検出用データとが示されている。バージョン番号はＥＣＭのバージョンを示す。コピー制御情報は、コンテンツのコピーの許否（ＣＯＰＹ　ＦＲＥＥ、ＮＥＴＷＯＲＫ　ＣＯＰＹ、ＣＯＰＹ　ＮＥＶＥＲ等）を示す。コンテンツ鍵は、スクランブル鍵とも呼ばれ、コンテンツの暗号化及び復号化用である。プライベートデータは、可変長の任意データが挿入される。改ざん検出用データはＥＣＭの改ざんを検出するために設定

される。なお、ＥＣＭの暗号化部分はＥＣＭ本体全体であり、ＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｍａｎａｇｅｍｅｎｔ Ｍｅｓｓａｇｅ）で配信されるワーク鍵等で暗号化される。

【００３４】

上記のコピー制御情報は、著作者又はコンテンツプロバイダ／サービスプロバイダ等によって設定される。ＣＯＰＹ　ＮＥＶＥＲは、コピー不可であって、視聴のみ可能であることを意味し、ネットワークにバインドされない。ＮＥＴＷＯＲＫ　ＣＯＰＹは、プライベートネットワーク内でのみ自由にコピー可能であることを意味し、ネットワークにバインドされる。ＣＯＰＹ　ＦＲＥＥは、自由にコピー可能であることを意味し、ネットワークにバインドされてもよいが、その必要はない。

【００３５】

また、本実施の形態では、コンテンツプロバイダ／サービスプロバイダは、上記のプライベートデータ内に、最大書き出し回数、書き出し先、書き出し経路等を設定することができる。これは、ネットワークにバインドされたコンテンツの書き出し及び再生表示を制御するための条件として用いられる。

【００３６】

記憶装置９０は、コンテンツ取り込み装置１００によって取り込まれたコンテンツ及び暗号変換されたコンテンツ鍵情報を記憶する。つまり、記憶装置９０は、ネットワークにバインドされた状態のコンテンツを記憶する。

【００３７】

例えば、記憶装置９０は、図２に示すようなホームサーバであり、ハードディスクを備え、ネットワーク上の装置からアクセス可能になっている。

コンテンツ利用装置１１０－１、１１０－２、１１０－３等は、コンテンツ取り込み装置１００又は記憶装置９０から、コンテンツおよび暗号変換されたコンテンツ鍵情報を取得し、既に取得済みのネットワーク鍵を用いて、暗号化されたコンテンツ鍵情報を復号してコンテンツ鍵を取り出し、コンテンツ鍵でコンテンツを復号してコンテンツを利用する。また、本コンテンツ利用システム１では、複数のコンテンツ利用装置１１０－１、１１０－２、１１０－３等をネットワーク１２０に接続することができる。

【００３８】

例えば、コンテンツ利用装置１１０－１、１１０－２、１１０－３等は、図２に示すように、デジタルＴＶ１１０－１、Ｄ－ＶＨＳ１１０－２、ＤＶＤレコーダ１１０－３、ＰＣ１１０－４などであり、コンテンツの表示、取り外し可能な蓄積メディア（Ｄ－ＶＨＳテープ、ＤＶＤ－ＲＡＭ、ＳＤメモリカード等）への記憶を行う機器である。あるいは、コンテンツ利用装置１１０は、これらの機能を複合した機器である。

【００３９】

ネットワーク１２０は、コンテンツ取り込み装置１００およびコンテンツ利用装置１１０－１、１１０－２、１１０－３等を相互に接続するネットワークであり、例えば、ＩＥＥＥ１３９４バス、ＩＥＥＥ８０２．３（１０／１００Ｂａｓｅ－Ｔ）、Ｂｌｕｅｔｏｏｔｈなどで実現される。

【００４０】

図３は、図１に示されるコンテンツ取り込み装置１００およびコンテンツ利用装置１１０の構成を示す機能ブロック図である。このコンテンツ利用システムは、ネットワークにバインドされたコンテンツをコンテンツ毎に識別できるようにし、当該コンテンツをネットワークにバインドしていない状態でコンテンツの書き出すことに制限を課するように構成されている。なお、コンテンツ利用装置１１０は、同等の構成を有するコンテンツ利用装置１１０－１、１１０－２、１１０－３等の１つの代表として図示している。また、本図には、記憶装置９０及びネットワーク１２０も併せて示されている。

【００４１】

コンテンツ取り込み装置１００は、入力部１０１と、分離部１０２と、コンテンツ鍵情報暗号変換部１０３と、コンテンツＩＤ生成部１０４と、多重化部１０５とを備えている。

【００４２】
入力部１０１は、デジタル放送のＭＰＥＧ－２トランスポートストリーム（ＴＳ）を入力ストリームとして取り込む。トランスポートストリームは、コンテンツ、ＥＣＭ、ＥＭＭ、ＰＳＩ（Ｐｒｏｇｒａｍ ＳＰｅｃｉｆｉｃ Ｉｎｆｏｒｍａｔｉｏｎ）などがパケット多重された構成となっており、トランスポートストリームパケット（ＴＳパケット）のヘッダ部のＰＩＤ（Ｐａｃｋｅｔ ＩＤ）で識別できるようになっている。
【００４３】
分離部１０２は、入力部１０１で取り込んだトランスポートストリームをコンテンツ、ＥＣＭ等に分離する。
具体的には、ＰＭＴ（Ｐｒｏｇｒａｍ ＭａＰ Ｔａｂｌｅ）と呼ばれるＰＳＩを参照して、ストリームを構成するエレメンタリのＰＩＤを取得する。そして、ＴＳパケットのヘッダ部のＰＩＤを参照し、コンテンツ、ＥＣＭ等のパケットを分離する処理を行う。
【００４４】
コンテンツ鍵情報暗号変換部１０３は、分離部１０２から受信したＥＣＭのパケットからＥＣＭセクションを再構成し、ＥＣＭを取り出し、当該ＥＣＭを暗号変換する。つまり暗号化されたＥＣＭを一旦復号して前述のネットワーク鍵を用いて復号されたＥＣＭを再暗号化する。
【００４５】
具体的には、ＥＣＭは、ＣＡＳのワーク鍵で暗号化されて放送波に多重された状態で配信される。コンテンツ鍵情報暗号変換部１０３は、ＣＡＳのワーク鍵で暗号化されたＥＣＭを復号し、コンテンツＩＤ生成部１０４にコンテンツＩＤの発行を要求し、要求に応じてコンテンツＩＤ生成部１０４で生成されたコンテンツＩＤを復号したＥＣＭに挿入した上で、ネットワーク鍵を用いて再度ＥＣＭを暗号化する。なお、ワーク鍵は、コンテンツの配信に先立ち、ＥＭＭによって放送波に多重されて配信されているのが一般的であるので、コンテンツ鍵情報暗号変換部１０３は、予めワーク鍵を取得することができる。
【００４６】
このように、コンテンツの暗号鍵であるコンテンツ鍵を含むＥＣＭにコンテンツＩＤを挿入することにより、コンテンツとコンテンツＩＤをセキュアにバインドしている。ここで、コンテンツＩＤを付与する単位は、分離部１０２によって識別されるイベントの単位でよい。ここでイベントは１つの放送番組に相当するコンテンツをいう。この場合、コンテンツ鍵情報暗号変換部１０３は、ＴＳ中のＳＩ（Ｓｅｒｖｉｃｅ Ｉｎｆｏｒｍａｔｉｏｎ）のＥＩＴ（Ｅｖｅｎｔ Ｉｎｆｏｒｍａｔｉｏｎ Ｔａｂｌｅ）からｅｖｅｎｔ＿ｉｄ等のイベント情報を取得することによってイベントを識別し、このイベント単位でコンテンツＩＤの生成を要求する。
【００４７】
コンテンツＩＤ生成部１０４は、コンテンツ鍵情報暗号変換部１０３からの要求に基づき、ユニークなコンテンツＩＤを発行する。具体的には、コンテンツＩＤ生成部１０４は、内部にカウンタを有し、コンテンツ鍵情報暗号変換部１０３からコンテンツＩＤ発行の要求を受ける度に現在のカウンタ値をコンテンツＩＤに割り当て、カウンタをインクリメントするといった処理を行う。
【００４８】
多重化部１０５は、分離部１０２から受け取ったコンテンツと、コンテンツ鍵情報暗号変換部１０３から受け取った暗号化されたＥＣＭとを、再度トランスポートストリームとして多重化する処理を行う。
【００４９】
記憶装置９０は、多重化部１０５から出力されるトランスポートストリームを記憶する。一方、コンテンツ利用装置１１０は、分離部１１１と、コンテンツ鍵情報復号部１１２と、書き出しコンテンツリスト管理部１１３と、書き出しコンテンツリスト蓄積部１１４と、コンテンツ出力制御部１１５と、コンテンツ復号部１１６と、コンテンツ出力選択部１１７と、コンテンツ出力部としてコンテンツ表示部１１８およびコンテンツ書き出し部１

１９とを備える。

【００５０】

分離部１１１は、コンテンツ利用装置１１０においてユーザからコンテンツ表示要求又はコンテンツ書き出し要求を受けた場合に、コンテンツ取り込み装置１００又は記憶装置９０から取得したトランスポートストリームからコンテンツと再暗号化ＥＣＭとを分離する。

【００５１】

コンテンツ鍵情報復号部１１２は、分離部１１１から再暗号化ＥＣＭを受信し、ネットワーク鍵を用いて再暗号化されたＥＣＭを復号する。その際、ユーザからのコンテンツ書き出し要求があった場合には、書き出しコンテンツリスト管理部１１３による書き出しについての判定結果が許可である場合にのみ、復号したコンテンツ鍵をコンテンツ復号部１１６に渡す。具体的には、コンテンツ鍵情報復号部１１２は、ネットワーク鍵を用いて再暗号化されたＥＣＭを復号し、そのＥＣＭに含まれるコンテンツＩＤを書き出しコンテンツリスト管理部１１３に渡し、該当コンテンツＩＤのコンテンツの書き出しを許可するか禁止するかを示す判定結果を受け取り、判定結果が許可である場合に、復号したコンテンツ鍵をコンテンツ復号部１１６に渡す。このように、コンテンツリスト管理部１１３おいて個々のコンテンツについて書き出しの許否を判定することにより、コンテンツをバインドしていない状態で無制限に外部に出力することができないようにしている。

【００５２】

また、ユーザからのコンテンツ表示要求があった場合のコンテンツ鍵情報復号部１１２の処理も、コンテンツ書き出し要求があった場合と同様である。ただし、書き出しコンテンツリスト管理部１１３から得られる判定結果は書き出しの許可又は禁止についての判定結果ではなくコンテンツの再生表示についての判定結果である。

【００５３】

書き出しコンテンツリスト管理部１１３は、書き出しコンテンツリスト蓄積部１１４に蓄積された書き出しコンテンツリスト（Ｍｏｖｅｄ　Ｃｏｎｔｅｎｔ　Ｌｉｓｔ、以下、ＭＣＬと記す）に基づいてコンテンツ出力を許可するか禁止するかの判定と、ＭＣＬの更新とを行う。ここで、ＭＣＬは、少なくとも既に書き出しがなされたコンテンツのコンテンツＩＤを含むリストである。コンテンツ出力許否判定は、コンテンツの書き出しの許否の判定と、コンテンツ再生表示の許否の判定とがある。

【００５４】

具体的には、書き出しコンテンツリスト管理部１１３は、コンテンツＩＤをコンテンツ鍵情報復号部１１２から受け取った場合、次の（Ａ）又は（Ｂ）等の処理によりコンテンツの書き出し許否の判定を行う。

【００５５】

（Ａ）受け取ったコンテンツＩＤが既にＭＣＬに登録されているか否かを判定し、登録されていなければ、ＭＣＬに当該コンテンツＩＤを追加して書き出しを許可し、既に登録されていれば、コンテンツの書き出しを禁止する。この場合、各コンテンツに対して書き出しを１回だけ許可し、２回目以降は禁止することができる。この場合のＭＣＬは、既に１回書き出したコンテンツのコンテンツＩＤリストとなる。ＭＣＬにコンテンツＩＤが登録されていないことが、コンテンツを書き出すための条件（書き出し条件）となる。

【００５６】

（Ｂ）受け取ったコンテンツＩＤが既にＭＣＬに登録されているか否かを判定し、登録されていなければ、ＭＣＬに当該コンテンツＩＤを登録し、予め定められた書き出し条件又はＭＣＬに従ってコンテンツ書き出しの許否を判定し、登録されていれば、当該コンテンツＩＤに対応する書き出し条件に従ってコンテンツの書き出しの許否を判定する。ここで、書き出し条件は、例えば、コンテンツの書き出し可能回数、書き出し先（どの蓄積メディアに書き出せるか）、書き出し経路（アナログ出力／デジタル出力など）等でよい。この場合、コンテンツ毎に、書き出し条件に従ってコンテンツの書き出しを制限することになる。コンテンツの書き出し可能回数は、例えばネットワーク１２０内でネットワーク鍵

を共有しているコンテンツ利用装置１１０の数である。
【００５７】
また、コンテンツリスト管理部１１３は、コンテンツの再生表示についての拒否の判定についても上記（Ａ）（Ｂ）と同様に判定するが、コンテンツの書き出し条件ではなくコンテンツの再生表示条件に従う。
【００５８】
また、書き出しコンテンツリスト管理部１１３は、書き出しコンテンツリスト蓄積部１１４のＭＣＬのハッシュ値をセキュアに管理する。これは、ＭＣＬをハードディスク等の非セキュアな領域に蓄積する場合に、不正なユーザによる改ざんの有無の検出を行い、その正当性を確保するためである。そのため書き出しコンテンツリスト管理部１１３は、ＭＣＬの内容が更新される度に、ＭＣＬのハッシュ値を計算し、計算結果を管理する。ハッシュ値のセキュアな管理方法の一例としては、ハード的に耐タンパ化されたセキュリティモジュールの内部にハッシュ値を格納する方法が挙げられる。
【００５９】
さらに、書き出しコンテンツリスト管理部１１３は、ＭＣＬの最大サイズ、あるいは、コンテンツＩＤ数やＭＣＬのサイズに関するしきい値を管理する。これは、ＭＣＬに掲載する最大コンテンツＩＤ数や最大バイト数などのしきい値を管理しておき、ＭＣＬがしきい値に達した場合は、ＭＣＬへの掲載の古いコンテンツＩＤの情報から削除する処理を行う。具体的には、書き出しコンテンツリスト管理部１１３は、次にＭＣＬへ書き込む位置を示すポインタを管理し、ＭＣＬが上限値に達した場合は、ポインタをＭＣＬの先頭に戻すことにより、古いコンテンツＩＤの情報から削除することが可能となる。
【００６０】
あるいは、コンテンツへのアクセス日時をＭＣＬのコンテンツ毎の情報として書き込んでおくことにより、アクセス頻度の少ない情報から削除（上書き）するようにすることもできる。
【００６１】
あるいは、上述のように自動的に削除するのではなく、ＭＣＬから削除する情報をユーザに選択させ、ユーザ操作により削除するようにしても良い。
書き出しコンテンツリスト蓄積部１１４は、ＭＣＬを蓄積しておく部であり、ハードディスク等によって実現される。
【００６２】
コンテンツ出力制御部１１５は、コンテンツ出力選択部１１７に対し、コンテンツ出力を制御するためのコンテンツ出力制御情報を出力する。具体的には、コンテンツ出力制御部１１５は、ユーザからのコンテンツ表示要求または書き出し要求に基づき、コンテンツをコンテンツ表示部１１８に出力するか、コンテンツ書き出し部１１９に出力するかを指定するためのコンテンツ出力制御情報を生成し、コンテンツ出力選択部１１７に送信する。
【００６３】
コンテンツ復号部１１６は、暗号化されたコンテンツを復号する。具体的には、コンテンツ鍵により暗号化されているコンテンツのＴＳパケットを、コンテンツ鍵情報復号部１１２から取得したコンテンツ鍵を用いて、順次復号する処理を行う。
【００６４】
コンテンツ出力選択部１１７は、コンテンツ出力制御部１１５から取得したコンテンツ出力制御情報に基づき、コンテンツの渡し先を制御する。具体的には、コンテンツ出力制御情報が表示を示す場合は、コンテンツをコンテンツ表示部１１８に送信し、コンテンツ出力制御情報が蓄積メディアへの書き出しを示す場合は、コンテンツをコンテンツ書き出し部１１９に送信する処理を行う。
【００６５】
コンテンツ表示部１１８は、コンテンツのＴＳパケットからＭＰＥＧ－２のエレメンタリストリームを再構成し、デコードし、コンテンツをモニターに出力する。
【００６６】

コンテンツ書き出し部１１９は、コンテンツを書き出すために必要な処理を行い、蓄積メディアに書き出す処理を行う。具体的には、コンテンツをメディアにバインドするために暗号変換したり、フォーマットを変換したり、といった処理を行う。

【００６７】

図５は、書き出しコンテンツリスト蓄積部１１４に蓄積され、書き出しコンテンツリスト管理部１１３で管理されるＭＣＬのデータ構成の一例を示す図である。このＭＣＬは、コンテンツ書き出し部１１９によって書き出されたコンテンツ及びコンテンツ表示部１１８により再生表示されたコンテンツを掲載したリストである。図示するように、このＭＣＬは、コンテンツＩＤに対応して書き出し回数、書き出し先、書き出し経路を含む。書き出し回数は、コンテンツ毎にコンテンツ書き出し部１１９によって蓄積メディアに何回書き出しを行ったかを示す。書き出し先は、ＤＶＤ－ＲＡＭ、Ｄ－ＶＨＳ、ＳＤカードなどの書き出しが許可される蓄積メディアを示す。書き出し経路は、アナログ出力、デジタル出力（圧縮／非圧縮）、出力画質（ＳＤ／ＨＤ）等の出力形態を示す。また、書き出しコンテンツリスト管理部１１３は、書き出し先、書き出し経路などの情報を、図４に示したＥＣＭ内のプライベートデータから取得してＭＣＬに設定してもよいし、放送波に含まれる情報（コンテンツ、ＥＣＭ、ＰＳＩ／ＳＩ等）から取得して設定しても良いし、本コンテンツ利用システムが予め保持している値を設定しても良い。

【００６８】

このように構成されたＭＣＬによれば、コンテンツＩＤに対して、既にコンテンツを書き出した回数がわかるため、書き出しコンテンツリスト管理部１１３において、１コンテンツ当たりの最大書き出し回数の範囲内に、コンテンツの書き出しを制限することが可能となる。

【００６９】

以上のように構成されたコンテンツ利用システム１の動作を、図６および図７に示すフローチャートを用いて説明する。

図６は、コンテンツ取り込み装置１００における、コンテンツ取り込み処理を示すフローチャートである。

【００７０】

入力部１０１は、放送波からトランスポートストリームを受信する（ステップＳ４０１）。

分離部１０２は、入力部１０１からトランスポートストリームを受け取り、ＴＳパケットのＰＩＤを参照して、コンテンツのＴＳパケットや、ＥＣＭ等のＴＳパケットを分離する（ステップＳ４０２）。コンテンツやＥＣＭのＴＳパケットを示すＰＩＤは、ＰＭＴに記述されているので、これを参照して、ＴＳパケットの分離を行う。

【００７１】

コンテンツ鍵情報暗号変換部１０３は、ＥＣＭのＴＳパケットを受け取り、ＥＣＭセクションを再構成し、ワーク鍵を用いて暗号化されたＥＣＭを復号する（ステップＳ４０３）。さらにコンテンツ鍵情報暗号変換部１０３は、復号されたＥＣＭ中のコピー制御情報がコピー禁止（ＣＯＰＹ　ＮＥＶＥＲ）である場合は、ネットワークにバインドしないので、以下の処理を行わない（コンテンツは再生表示可能）。ＮＥＴＷＯＲＫ　ＣＯＰＹである場合は、ネットワークにバインドするため以下を続行する。ＣＯＰＹ　ＦＲＥＥである場合は、必ずしもネットワークにバインドする必要はないが、書き出し回数を無制限としてネットワークにバインドしてもよい。

【００７２】

コンテンツ鍵情報暗号変換部１０３は、コンテンツＩＤ生成部１０４に対してコンテンツＩＤ生成要求を送る。コンテンツＩＤ生成部１０４はこれを受けて、コンテンツＩＤを生成する（ステップＳ４０４）。

【００７３】

コンテンツＩＤ生成部１０４は、生成したコンテンツＩＤをコンテンツ鍵情報暗号変換部１０３に送る。コンテンツ鍵情報暗号変換部１０３は、取得したコンテンツＩＤをＥＣＭ

に埋め込む（ステップＳ４０５）。具体的には、コンテンツＩＤ生成部１０４は、内部に保持するカウンタを用いてコンテンツＩＤを生成し、これをコンテンツ鍵情報暗号変換部１０３に送る。コンテンツ鍵情報暗号変換部１０３は、受け取ったコンテンツＩＤを、ＥＣＭの特定のフィールドに設定する。一例としては、図４に示すＥＣＭのプライベートデータ部に挿入する方法が挙げられる。

【００７４】

コンテンツ鍵情報暗号変換部１０３は、ＥＣＭをネットワーク鍵で再暗号化する（ステップＳ４０６）。具体的には、コンテンツ鍵情報暗号変換部１０３は、ネットワークで予め共有された暗号鍵を内部で保持し、これを用いて、コンテンツＩＤを埋め込んだＥＣＭを再暗号化する。さらに、このように暗号化されたＥＣＭをＴＳパケット化して、多重化部１０５に渡す。

【００７５】

多重化部１０５は、分離部１０２から受け取ったコンテンツのＴＳパケットと、コンテンツ鍵情報暗号変換部１０３から受け取った暗号変換後のＥＣＭのＴＳパケットとを多重化する（ステップＳ４０７）。

【００７６】

多重化後のコンテンツとＥＣＭは記憶装置９０に格納される。あるいは、記憶装置９０に格納されると同時にコンテンツ利用装置１１０に入力される。

このように、コンテンツ取り込み装置１００では、ＥＣＭの暗号が変換されることにより、ネットワークにバインドされたコンテンツが生成されると共に、コンテンツＩＤがＥＣＭに設定され、コンテンツと多重化される。

【００７７】

一方、図７は、コンテンツ利用装置１１０における、コンテンツ書き出し処理を示すフローチャートである。

分離部１１１において、コンテンツ取り込み装置１００からから受け取ったトランスポートストリーム又は記憶装置９０から読み出されたトランスポートストリームから、コンテンツとＥＣＭを分離する（ステップＳ５０１）。具体的には、トランスポートストリームのＴＳパケットのヘッダ部にあるＰＩＤを参照し、それぞれのＰＩＤに該当するＴＳパケットを分離する処理を行う。

【００７８】

コンテンツ鍵情報復号部１１２は、分離部１１１からＥＣＭのＴＳパケットを受け取り、ＥＣＭセクションを再構成し、再暗号化されたＥＣＭを取得する。ＥＣＭの暗号化部分を予め取得してあるネットワーク鍵で復号する（ステップＳ５０２）。

【００７９】

コンテンツ鍵情報復号部１１２は、復号したＥＣＭに埋め込まれているコンテンツＩＤを読み出す（ステップＳ５０３）。コンテンツ鍵情報復号部１１２は、該当コンテンツが書き出しを許可されているか否かを確認するため、読み出したコンテンツＩＤを書き出しコンテンツリスト管理部１１３に渡す。

【００８０】

書き出しコンテンツリスト管理部１１３は、書き出しコンテンツリスト蓄積部１１４からＭＣＬを読み出す（ステップＳ５０４）。書き出しコンテンツリスト管理部１１３は、まず、トランスポートストリームに含まれる情報（コンテンツ、ＥＣＭ、ＰＳＩ／ＳＩ等）から、または、システムが予め規定しているパラメータからコンテンツの書き出し先、書き出し経路の条件を取得し、ユーザが指定した書き出し先、書き出し経路が条件を満たすかどうか確認する（ステップＳ５０５）。例えば、ユーザが書き出し先を「Ｄ－ＶＨＳ」と指定し、コンテンツ利用装置１１０で予め備えられている書き出し先が「Ｄ－ＶＨＳ」である場合は、該当コンテンツをＤ－ＶＨＳへ書き出すことができるが、コンテンツ利用装置１１０で予め備えられている書き出し先が「ＳＤカード」であった場合は、書き出すことができない。書き出し経路についても同様に、ユーザの指定が、コンテンツ利用装置１１０で備えられている書き出し経路を満たさない限り、コンテンツを蓄積メディアに書

き出すことができない。

【００８１】

さらに、書き出しコンテンツリスト管理部１１３は、コンテンツ鍵情報復号部１１２から受け取ったコンテンツＩＤがＭＣＬに存在するか否かを判定する（ステップＳ５０６）。なお、書き出しコンテンツリスト蓄積部１１４にＭＣＬ自体が無かった場合（初期化されていない場合）は、ＭＣＬを生成する（初期化）する。

【００８２】

ステップＳ５０６において、ＮＯの場合、すなわちコンテンツＩＤがＭＣＬに存在しない場合は、ＭＣＬを更新し、書き出しコンテンツリスト蓄積部１１４に蓄積する処理を行う（ステップＳ５０７）。この場合、該当コンテンツを書き出し可能であると判定している。

【００８３】

そして、該当コンテンツを書き出したことを記録するため、該当コンテンツＩＤ、書き出し回数、書き出し先、書き出し経路をＭＣＬに追加し、ＭＣＬのハッシュを再計算して、ＭＣＬを書き出しコンテンツリスト蓄積部１１４に蓄積すると共に、書き出しコンテンツリスト管理部１１３で保持しているハッシュ値を、再計算したＭＣＬのハッシュ値で置き換える。

【００８４】

コンテンツ鍵情報復号部１１２は、ＥＣＭからコンテンツ鍵を取り出し、コンテンツ鍵をコンテンツ復号部１１６に渡すと共に、コンテンツ出力制御部１１５に対し、確認した書き出し先、書き出し経路で、当該コンテンツをコンテンツ書き出し部１１９へ渡すように指示を行う（ステップＳ５０８）。これにより、コンテンツ出力制御部１１５は、コンテンツ出力選択部１１７に対して、指定された書き出し先、書き出し経路でコンテンツを書き出すように制御する。

【００８５】

コンテンツ復号部１１６は、分離部１１１から取得したＴＳパケットを、コンテンツ鍵情報復号部１１２から取得したコンテンツ鍵で復号（デスクランブル）する（ステップＳ５０９）。

【００８６】

コンテンツ出力選択部１１７は、コンテンツ出力制御部１１５の制御に基づき、指定された書き出し先、書き出し経路で、コンテンツを書き出すためコンテンツ書き出し部１１９へコンテンツを渡す。

【００８７】

コンテンツ書き出し部１１９は、コンテンツを蓄積メディアに書き出す（ステップＳ５１０）。具体的には、ＤＶＤ－ＲＡＭ、Ｄ－ＶＨＳ等の蓄積メディアに対応した形式で、コンテンツを暗号化したり、フォーマット変換したりして、蓄積メディアにコンテンツを書き出す。

【００８８】

ステップＳ５０６において、ＹＥＳの場合、すなわちコンテンツＩＤがＭＣＬに存在する場合は、ＭＣＬの該当コンテンツＩＤに関する情報を用いて、書き出し可否の確認を行う（ステップＳ５１１）。具体的には、ＭＣＬには、コンテンツＩＤ毎に書き出し回数、書き出し先、書き出し経路などが記録されるようになっているため、これらを参照して、書き出し可能かどうかの確認を行う。

【００８９】

例えば、コンテンツ毎に書き出し許容回数が「３」であり、書き出そうとするコンテンツのコンテンツＩＤが図５における「ＣＯＮＴＥＮＴ－ＩＤ－１１１１１」である場合、書き出し回数が「１」であるので、残り２回は書き出し可能であるため書き出し可能と判定される。このとき、書き出し先と書き出し経路については、ＭＣＬの内容が「－」、すなわち、書き出し先と書き出し経路については限定しないことを示しているため、ユーザの指定した書き出し先、書き出し経路での書き出しが可能である。また、コンテンツＩＤが

「ＣＯＮＴＥＮＴ－ＩＤ－２２２２２」、ユーザが指定した書き出し先が「ＤＶＤ－ＲＡＭ」である場合、書き出し回数が「２」、書き出し先が「ＤＶＤ－ＲＡＭ」であるので、書き出し可能と判定される。このとき、例えばユーザが指定した書き出し先が「ＳＤカード」であった場合は、書き出し回数の制限を満たしている場合でも、書き出し先の制限を満たさないので、書き出し不可と判定される。また、コンテンツＩＤが、「ＣＯＮＴＥＮＴ－ＩＤ－８８８８８」、ユーザが指定した書き出し経路が「Ｄｉｇｉｔａｌ（ＳＤ）」である場合は、書き出し回数と書き出し経路の制限を共に満たすため、書き出し可能と判定されるが、ユーザが指定した書き出し経路が「Ｄｉｇｉｔａｌ（ＨＤ）」であった場合は、書き出し経路の制限を満たさないので、書き出し不可と判定される。さらに、「ＣＯＮＴＥＮＴ－ＩＤ－７７７７７」である場合は、既に書き出し回数が「３」であるので、書き出し不可と判定される。

【００９０】

ステップＳ５１１において、ＹＥＳの場合、すなわち書き出し可能と判定された場合は、ＭＣＬを更新、蓄積する（ステップＳ５０７）。ステップＳ５０７以降の処理の詳細については前述の通りであるので、以降は省略する。

【００９１】

ステップＳ５１１において、ＮＯの場合、すなわち書き出し不可と判定された場合は、コンテンツ書き出し処理を終了する。

このように、本コンテンツ利用システム１では、ネットワークバインドされたコンテンツにコンテンツＩＤを付与し、コンテンツを書き出す際に、ＭＣＬで書き出し確認を行うことにより、無制限なコンテンツの書き出しに制限を課するようになっている。

【００９２】

また、図７では、コンテンツ利用装置１１０における、コンテンツ書き出し処理のフローチャートを示したが、図８では、コンテンツ再生（表示）処理を示すフローチャートが示されている。

【００９３】

図８において、ステップＳ６０１～Ｓ６０６の処理については、図７に示したコンテンツ書き出し処理と同様であるので、ここでは省略する。

ステップＳ６０６において、ＮＯの場合、すなわちＭＣＬに該当コンテンツＩＤが存在しない場合は、該当のコンテンツを書き出していないので、再生処理可能と判定し、コンテンツ鍵情報復号部１１２は、ＥＣＭからコンテンツ鍵を取り出し、コンテンツ復号部１１６に渡す処理を行う（ステップＳ６０８）。

【００９４】

コンテンツ復号部１１６は、分離部１１１から取得したＴＳパケットを、コンテンツ鍵情報復号部１１２から取得したコンテンツ鍵で復号（デスクランブル）する（ステップＳ６０９）。

【００９５】

コンテンツ出力選択部１１７は、コンテンツ出力制御部１１５の制御に基づき、コンテンツを表示するためのコンテンツ表示部１１８へコンテンツを渡す。

コンテンツ表示部１１８は、コンテンツをＴＶ等に出力する（ステップＳ６１０）。

【００９６】

ステップＳ６０６において、ＹＥＳの場合、すなわちＭＣＬに該当コンテンツＩＤが存在する場合は、ＭＣＬの該当コンテンツＩＤに関する情報を用いて再生可否の確認を行う（ステップＳ６０７）。具体的には、書き出し回数が書き出し上限回数に達しているか否かを確認し、書き出し上限回数に達していない場合は再生可、書き出し上限回数に達している場合は再生不可と判定する。

【００９７】

ステップＳ６０７において、ＹＥＳの場合、すなわち再生可の場合は、ステップＳ６０８以降を実行する。

ステップＳ６０７において、ＮＯの場合、すなわち再生不可の場合は、コンテンツ再生処

理を終了する。

【００９８】

このように、本コンテンツ利用システム１では、蓄積メディアに書き出したコンテンツであっても、ネットワーク内にコンテンツのコピーが存在する可能性があるため、書き出したコンテンツの表示（再生）処理時においても、ＭＣＬを用いてコンテンツの再生が可能か否かを確認することで、利用に制限を課するようにしている。

【００９９】

ところで、電源断やユーザキャンセル等により、書き出し処理が中断（失敗）してしまう場合が発生しうる。そのため、本コンテンツ利用システム１では、このような場合において、書き出し処理を再開することができるようにしている。具体的には、図３において、コンテンツ鍵情報復号部１１２において、スクランブル単位（例えば、ＥＣＭに含まれるコンテンツ鍵が更新される単位）にＩＤ（以降、スクランブルＩＤと記す）を付与し、コンテンツ復号部１１６はコンテンツ鍵と前記スクランブルＩＤを受け取り、どこまでコンテンツ書き出し部１１９にコンテンツを渡したか、すなわち、どこまで蓄積メディアへの書き出しが成功したかを保持しておく。キャンセルが発生し、書き出し処理を再開する場合には、コンテンツ復号部１１６は、保持しているスクランブルＩＤをコンテンツ鍵情報復号部１１２に送信することにより、該当するスクランブルＩＤから処理を再開することができるようにしている。

【０１００】

この処理について、図９および図１０に示すフローチャートを用いて説明する。

図９は、コンテンツの蓄積メディアへの書き出し処理を示すフローチャートである。同図では、書き出しを開始し、中断（キャンセルやポーズ）するまで、及び終了するまでの処理を示している。

【０１０１】

コンテンツの書き出し処理が開始されると、書き出しコンテンツリスト管理部１１３は、書き出すコンテンツのコンテンツＩＤを仮登録する（ステップＳ７０１）。

【０１０２】

コンテンツ鍵情報復号部１１２は、書き出し処理中断（キャンセル）原因が発生しているかどうかをチェックする（ステップＳ７０２）。処理中断でない場合はステップＳ７０３を実行し、処理中断の場合は、コンテンツ書き出し処理を終了する。電源断の場合も当然に終了する。

【０１０３】

ステップＳ７０３では、コンテンツを全スクランブル単位分出力したか否かを判定する。全スクランブル単位を出力していない場合は、ステップＳ７０４を実行し、全スクランブル単位を出力した場合は、ステップＳ７０９を実行する。

【０１０４】

コンテンツ鍵情報復号部１１２は、スクランブル単位毎にスクランブルＩＤを付与する（ステップＳ７０４）。具体的には、スクランブル単位毎に単調増加するＩＤを付与することにより、コンテンツ復号部１１６あるいはコンテンツ書き出し部１１９が、どこまで書き出ししたかを識別するＩＤとして用いることができる。また、最後に付与したスクランブルＩＤを、最終送出スクランブルＩＤとして、内部に保持する。

【０１０５】

コンテンツ鍵情報復号部１１２は、ＥＣＭからコンテンツ鍵を読み出し、コンテンツ復号部１１６に、コンテンツ鍵とスクランブルＩＤとを渡す（ステップＳ７０５）。ここで、複数のコンテンツの書き出し処理が中断される場合を考慮し、スクランブルＩＤと共に、書き出すコンテンツのコンテンツＩＤを渡すようにしてもよい。

【０１０６】

コンテンツ復号部１１６は、コンテンツ鍵とスクランブルＩＤを受信する（ステップＳ７０６）。

コンテンツ復号部１１６は、暗号化されたコンテンツをコンテンツ鍵で復号し、書き出し

が完了したスクランブル単位のスクランブルＩＤを内部に保持する（ステップＳ７０７）。

【０１０７】

コンテンツ書き出し部１１９は、コンテンツを書き出す（ステップＳ７０８）。

ステップＳ７０３でコンテンツを全スクランブル単位分出力したと判定した場合は、書き出しコンテンツリスト管理部１１３は、書き出すコンテンツのコンテンツＩＤをＭＣＬへ本登録する（ステップＳ７０９）。

【０１０８】

なお、ここではコンテンツ復号部１１６で暗号化されたコンテンツを復号した時点で、スクランブルＩＤを内部に保持するようにしたが、コンテンツ書き出し部１１９からコンテンツを書き出し、蓄積メディアに正常に書き込まれた旨の通知を受けてから、スクランブルＩＤを内部に保持するようにしても良い。

【０１０９】

図１０は、処理の中断が発生後、処理を再開（継続）する処理を示している。同図の処理は、ＭＣＬに仮登録されたコンテンツＩＤが発見された場合や、ユーザにより再開要求を受けた場合等に開始する。

【０１１０】

同図において、コンテンツ復号部１１６は、コンテンツ鍵情報復号部１１２に、保持しているスクランブルＩＤを送信する（ステップＳ８０１）。

コンテンツ鍵情報復号部１１２は、スクランブルＩＤを受信する（ステップＳ８０２）。

【０１１１】

コンテンツ鍵情報復号部１１２は、保持している最終送出スクランブルＩＤと、コンテンツ復号部１１６から受け取ったスクランブルＩＤを比較する（ステップＳ８０３）。具体的には、コンテンツ復号部１１６から受け取ったスクランブルＩＤと、最終送出スクランブルＩＤの差分を求め、差分が予め設定された　値以下であるか否かを判定することで、不正な書き出しを防止する。

【０１１２】

ステップ８０３において、ＹＥＳの場合、すなわち差分が　値以下の場合は、書き出し処理の再開を許可し、コンテンツ書き出し処理を再開する（ステップＳ８０４）。なお、コンテンツ書き出し処理の再開後の動作については、図９で説明しているので、ここでは省略する。

【０１１３】

ステップ８０３において、ＮＯの場合、すなわち差分が　値より大きい場合は、コンテンツ書き出し処理を中止する（ステップＳ８０５）。

このように、本コンテンツ利用システム１では、コンテンツの書き出しに際して、書き出しの進捗を識別するためのスクランブルＩＤを付与するようにしているので、コンテンツ書き出し時の電源断、ユーザによる中断などがあった場合でも、セキュリティ上、安全に再開することができるようになっている。

【０１１４】

（実施の形態２）

以下、本発明の実施の形態２について、図面を用いて詳細に説明する。

図１１は、本発明の実施の形態２に係るコンテンツ利用システム２の構成を示すブロック図である。なお、本図において、図３に示した実施の形態１のコンテンツ利用システム１と同様の構成要素については、図３において既に説明しているので、図３と同様の符号を付して以下の説明を省略する。

【０１１５】

図１１に示すコンテンツ利用システム２では、コンテンツ取り込み装置１００は本発明の実施の形態１に挙げたコンテンツ利用システム１と同様の構成であるが、コンテンツ利用装置１１０αが、さらに書き出しコンテンツリスト同期部９０１を備えており、ネットワーク接続された他のコンテンツ利用装置１１０αと通信を行い、複数のコンテンツ利用装

置１１０α間でＭＣＬの同期を行うことを特徴とする。

【０１１６】

書き出しコンテンツリスト同期部９０１は、他のコンテンツ利用装置１１０αとの間でＭＣＬの同期情報を送受信することでＭＣＬの同期を取り、その結果を書き出しコンテンツリスト管理部１１３に通知する。具体的には、コンテンツの書き出しを行い、ＭＣＬを更新したタイミングで、書き出しコンテンツリスト管理部１１３は、書き出しコンテンツリスト同期部９０１に対し、更新したコンテンツＩＤに関する同期情報を渡す。書き出しコンテンツリスト同期部９０１は、この同期情報をネットワーク接続された他のコンテンツ利用装置１１０αに送信する。この同期情報を受信した他のコンテンツ利用装置１１０αの書き出しコンテンツリスト同期部９０１は、同期情報を書き出しコンテンツリスト管理部１１３に渡し、この情報を書き出しコンテンツリスト蓄積部１１４のＭＣＬに反映することにより、ＭＣＬの同期を確保する。同期する情報（同期情報）の一例としては、書き出したコンテンツＩＤを含む、ＭＣＬに記録された情報である。また、同期方法の一例としては、ネットワーク上に同期情報をブロードキャストする方法が挙げられる。

【０１１７】

図１２は、書き出しコンテンツリスト同期部９０１が、ネットワーク接続された他のコンテンツ利用装置１１０αの書き出しコンテンツリスト同期部９０１とＭＣＬの同期をとる場合のシーケンス図である。本図では、ＭＣＬの更新元（ＭＣＬを更新し、同期情報をブロードキャストするコンテンツ利用装置１１０α）を第１のコンテンツ利用装置１１０α、ＭＣＬの更新先（ブロードキャストされた同期情報を受信し、ＭＣＬを更新するコンテンツ利用装置１１０α）を第２のコンテンツ利用装置１１０βとする。なお、ＭＣＬの更新先に相当するコンテンツ利用装置１１０αは、複数存在する可能性があるが、第２のコンテンツ利用装置１１０βをその代表として示している。

【０１１８】

第１のコンテンツ利用装置１１０αの書き出しコンテンツリスト管理部１１３は、コンテンツを書き出す場合、コンテンツ鍵情報復号部１１２から該当コンテンツのコンテンツＩＤを取得し、書き出しコンテンツリスト蓄積部１１４から読み出したＭＣＬを更新する（ステップＳ１００１）。具体的には、コンテンツＩＤが「ＣＯＮＴＥＮＴ－ＩＤ－１２３４５」であるコンテンツを書き出した場合、図１３に示すように、第１のコンテンツ利用装置１１０αが保持するＭＣＬには、「ＣＯＮＴＥＮＴ－ＩＤ－１２３４５」のコンテンツＩＤに関する情報（コンテンツＩＤ、書き出し回数など）が追加されている。このとき、図１４に示したように、第２のコンテンツ利用装置１１０βが保持するＭＣＬには、第１のコンテンツ利用装置１１０αが「ＣＯＮＴＥＮＴ－ＩＤ－１２３４５」なるコンテンツＩＤのコンテンツを書き出したことは通知されていないため、「ＣＯＮＴＥＮＴ－ＩＤ－１２３４５」のレコードは存在しない。

【０１１９】

なお、図１３に示すＭＣＬでは、コンテンツの書き出し回数を示す情報に関して、書き出しを行った回数（書き出し回数）と、書き出し可能な最大回数（最大書き出し回数）が記録されるようになっている。よって、コンテンツの再生を制御する場合に、書き出し回数が最大書き出し回数に達していない間は、該当コンテンツの再生が可能であるが、最大書き出し回数に達した場合は、該当コンテンツの再生を不可とする制御を行う。また、ここでは書き出し回数として、既に書き出した回数を記録するようにしたが、書き出し可能な残り回数を記録するようにし、書き出しを行う都度、書き出し回数を減算していくようにしても良い。この場合は、書き出し回数が０となった時点で、該当コンテンツの書き出し及び再生が不可となる。

【０１２０】

第１のコンテンツ利用装置１１０αの書き出しコンテンツリスト管理部１１３は、更新したコンテンツＩＤに関する情報を、書き出しコンテンツリスト同期部９０１に通知する（ステップＳ１００２）。具体的には、第１のコンテンツ利用装置１１０αの書き出しコンテンツリスト管理部１１３は、図１３に示す第１のコンテンツ利用装置１１０αのＭＣＬ

において、コンテンツＩＤが「ＣＯＮＴＥＮＴ－ＩＤ－１２３４５」のレコード全てを書き出しコンテンツリスト同期部９０１に通知する。

【０１２１】

第１のコンテンツ利用装置１１０αの書き出しコンテンツリスト同期部９０１は、書き出しコンテンツリスト管理部１１３から受け取った、コンテンツＩＤが「ＣＯＮＴＥＮＴ－ＩＤ－１２３４５」に関する情報から、同期情報を生成する（ステップＳ１００３）。同期情報の一例としては、図１５に示すような同期情報１３０１が挙げられる。同期情報１３０１は以下の情報から構成されている。

【０１２２】

セッションＩＤ（ＳＥＳＳＩＯＮ－ＩＤ）は、コンテンツ利用装置１１０α毎に同期情報を生成する度に設定される。具体的には、カウンタなどで実現され、同期情報を生成する度に１を加算されるＩＤである。

【０１２３】

コンテンツ利用装置ＩＤ（ＴＥＲＭＩＮＡＬ－ＩＤ）は、コンテンツ利用装置１１０αが内部に保持し、コンテンツ利用装置１１０αを識別するためのＩＤであり、例えば、複数のコンテンツ利用装置１１０αにおいて、同時に同一コンテンツＩＤのコンテンツを書き出し、双方の同期情報がブロードキャストされた場合などに、両者を正確に区別するための情報として用いられる。

【０１２４】

コンテンツＩＤ（ＣＯＮＴＥＮＴ－ＩＤ）は、書き出したコンテンツのコンテンツＩＤである。

書き出し回数、書き出し先、書き出し経路は、基本的にＭＣＬの情報と同一である。なお、同期情報としてＭＣＬそのものを用いても良いが、以下の説明では、同期情報として、図１５に示す同期情報１３０１を用いる。

【０１２５】

次に、第１のコンテンツ利用装置１１０αの書き出しコンテンツリスト同期部９０１は、生成した同期情報１３０１を送信する（ステップＳ１００４）。具体的には、第１のコンテンツ利用装置１１０αの書き出しコンテンツリスト同期部９０１は、同期情報１３０１をネットワークにブロードキャストする。

【０１２６】

第２のコンテンツ利用装置１１０βの書き出しコンテンツリスト同期部９０１は、ブロードキャストされた同期情報１３０１を受信し、書き出しコンテンツリスト管理部１１３に対し、ＭＣＬを読み出すよう要求を行う。（ステップＳ１００５）。

【０１２７】

書き出しコンテンツリスト蓄積部１１４からＭＣＬを読み出し、第２のコンテンツ利用装置１１０βの書き出しコンテンツリスト管理部１１３は、ＭＣＬのハッシュを計算し、書き出しコンテンツリスト管理部１１３が保持している八ッシュ値と比較して、その正当性を確認し、その内容を書き出しコンテンツリスト同期部９０１に渡す（ステップＳ１００６）。なお、ＭＣＬが書き出しコンテンツリスト蓄積部１１４に存在しない場合は、ＭＣＬを生成（初期化）する。

【０１２８】

第２のコンテンツ利用装置１１０βの書き出しコンテンツリスト同期部９０１は、セッションＩＤやコンテンツ利用装置ＩＤ等を確認し、書き出しコンテンツリスト管理部１１３から受け取ったＭＣＬの内容と、同期情報１３０１とを比較し、同期情報１３０１をＭＣＬに反映するかどうかの判定を行う（ステップＳ１００７）。具体的には、同期情報１３０１の内容が、ＭＣＬの内容に含まれていないか、あるいは、更新されていないかを判定することによって行われる。

【０１２９】

ステップＳ１００７において、ＹＥＳの場合、すなわちＭＣＬを更新する必要があると判定された場合には、書き出しコンテンツリスト同期部９０１は、書き出しコンテンツリス

ト管理部１１３に同期情報１３０１の内容を通知し、書き出しコンテンツリスト管理部１１３は、ＭＣＬを同期情報１３０１の内容で更新する（ステップＳ１００８）。具体的には、図１４に示した第２のコンテンツ利用装置１１０βの保持するＭＣＬの内容が、図１３に示した第１のコンテンツ利用装置１１０αが保持するＭＣＬの内容に一致するよう同期される。

【０１３０】

第２のコンテンツ利用装置１１０βの書き出しコンテンツリスト管理部１１３は、ＭＣＬのハッシュを再計算し、ハッシュ値を内部で保持し、ＭＣＬを書き出しコンテンツリスト蓄積部１１４に書き込む（ステップＳ１００９）。

【０１３１】

ステップＳ１００７において、ＮＯの場合、すなわちＭＣＬを更新する必要がないと判定された場合には、本同期処理を終了する。具体的には、同期情報１３０１は複数回繰り返しブロードキャストされる可能性があるため、同期情報１３０１のセッションＩＤと同期情報送信元のコンテンツ利用装置ＩＤを参照して、複数回同じ同期情報１３０１を受信した場合には、不要な同期情報１３０１を破棄する処理を行う。

【０１３２】

なお、コンテンツ取り込み装置１００におけるコンテンツ取り込み処理、および、コンテンツ利用装置１１０αにおけるコンテンツ書き出し処理、および、コンテンツ利用装置１１０αにおけるコンテンツ再生処理については、本発明の実施の形態１と同様であり、既に説明しているため、ここでは説明を省略する。

【０１３３】

このように、本コンテンツ利用システム２では、ネットワーク上の複数のコンテンツ利用装置１１０α間でＭＣＬを同期するようにしている。そのため、本発明の実施の形態１で示したコンテンツ利用システム１が、書き出し可能なコンテンツ数などの制限をコンテンツ利用装置１１０α毎に課していたのに対し、ネットワーク全体、すなわち複数のコンテンツ利用装置１１０α全体に対して課するようにすることができる。

【０１３４】

（実施の形態３）

以下、本発明の実施の形態３について、図面を用いて詳細に説明する。

図１６は、本発明の実施の形態３に係るコンテンツ利用システム３の構成を示すブロック図である。なお、本図において、図３に示した実施の形態１のコンテンツ利用システム１と同様の構成要素については、図３において既に説明しているので、図３と同様の符号を付して以下の説明を省略する。

【０１３５】

図１６に示すコンテンツ利用システム３は、本発明の実施の形態１に挙げたコンテンツ利用システム１に対して、コンテンツ取り込み装置１００が、さらに書き出しコンテンツリスト管理部１４０１と、書き出しコンテンツリスト蓄積部１４０２と、コンテンツＩＤ受信部１４０３とを備え、コンテンツ利用装置１１０ｂが、分離部１１１と、コンテンツ鍵情報復号部１１２と、コンテンツ出力制御部１１５と、コンテンツ復号部１１６と、コンテンツ出力選択部１１７と、コンテンツ出力部としてコンテンツ表示部１１８およびコンテンツ書き出し部１１９と、コンテンツＩＤ送信部１４０４とを備えており、コンテンツ取り込み装置１００がＭＣＬを管理し、コンテンツ利用装置１１０ｂは、コンテンツを書き出したり、表示（再生）したりする場合において、コンテンツ取り込み装置１００に書き出し可否を問い合わせ、コンテンツ取り込み装置１００での書き出し可否判定の結果に基づいて、コンテンツの書き出しおよび表示を制御することを特徴とする。

【０１３６】

また、コンテンツ利用システム３で管理するＭＣＬは、コンテンツ利用システム３に取り込んだコンテンツに付与したコンテンツＩＤをＭＣＬに全て登録し、ＭＣＬの内、書き出したコンテンツのコンテンツＩＤのみにマーキングをするようにしている。そのため、コンテンツＩＤ生成部１０４は、新たにコンテンツを取り込む場合にコンテンツＩＤを生成

し、書き出しコンテンツリスト管理部１４０１にコンテンツＩＤを通知する必要がある。

【０１３７】

コンテンツ取り込み装置１００における書き出しコンテンツリスト管理部１４０１は、書き出しコンテンツリスト蓄積部１４０２に蓄積しているＭＣＬを読み出し、ＭＣＬの参照、更新処理等を行う。具体的には、ＭＣＬに登録するコンテンツＩＤをコンテンツＩＤ生成部１０４から受け取り、ＭＣＬにコンテンツＩＤを登録したり、書き出すコンテンツのコンテンツＩＤをコンテンツ利用装置１１０ｂから受けた場合に、書き出し可否を判定し、ＭＣＬを更新する、といった処理を行う。また、ＭＣＬが書き出しコンテンツリスト蓄積部１４０２に蓄積されていない場合は、ＭＣＬを新たに生成し、初期化する。なお、ＭＣＬのハッシュを計算し、セキュアに管理する方法については、本発明の実施の形態１において説明しているので、ここでは記述を省略する。

【０１３８】

コンテンツ取り込み装置１００における書き出しコンテンツリスト蓄積部１４０２は、ＭＣＬを蓄積しておく部であり、ハードディスク等によって実現される。

【０１３９】

コンテンツ取り込み装置１００におけるコンテンツＩＤ受信部１４０３は、コンテンツ利用装置１１０ｂのコンテンツＩＤ送信部１４０４から、書き出しあるいは再生するコンテンツのコンテンツＩＤを受信し、コンテンツＩＤを書き出しコンテンツリスト管理部１４０１に渡し、書き出しコンテンツリスト管理部１４０１から受け取った書き出し可否判定結果をコンテンツ利用装置１１０ｂのコンテンツＩＤ送信部１４０４に送信する処理を行う。

【０１４０】

コンテンツ利用装置１１０ｂにおけるコンテンツＩＤ送信部１４０４は、コンテンツ鍵情報復号部１１２から書き出しまたは再生を行うコンテンツのコンテンツＩＤを受信し、コンテンツＩＤをコンテンツ取り込み装置１００のコンテンツＩＤ受信部１４０３に送信し、コンテンツ取り込み装置１００での書き出し可否判定の結果を受信し、コンテンツ鍵情報復号部１１２に渡すといった処理を行う。

【０１４１】

また、本発明の実施の形態１におけるコンテンツ利用システム１、および、本発明の実施の形態２におけるコンテンツ利用システム２では、コンテンツＩＤをＥＣＭに設定する例を示したが、ここではＥＣＭ（コンテンツ鍵情報）以外の情報に設定する場合を示す。ＥＣＭ以外の情報の一例として、コンテンツＩＤをＰＭＴに設定したり、ＰｒｉｖａｔｅセクションとしてコンテンツＩＤを設定し、ＰＭＴからＰＩＤでポインティングする等の方法が挙げられる。ＰＭＴにコンテンツＩＤを設定する一例として、図１７では、ＰＭＴのｄｅｓｃｒｉＰｔｏｒ部の第１ループ部に、コンテンツＩＤを設定できるように規定されたｃｏｎｔｅｎｔ＿ｉｄ＿ｄｅｓｃｒｉＰｔｏｒを挿入する場合を示している。ＰＭＴのｄｅｓｃｉＰｔｏｒ部には、システム毎に規定される任意のディスクリプタが設定できるようになっており、デジタルコピーに関する情報を記したデジタルコピー制御記述子や、ＣＡＳの限定受信方式記述子などが挿入されたりする。本コンテンツ利用システムでは、このｄｅｓｃｒｉＰｔｏｒ部に、新たにｃｏｎｔｅｎｔ＿ｉｄ＿ｄｅｓｃｒｉＰｔｏｒを規定し、この中のｃｏｎｔｅｎｔ＿ｉｄフィールドにコンテンツＩＤを設定するようにしている。ちなみに、ディスクリプタを第１ループ部に設定するか、第２ループ部に設定するかは、システムによって任意であるが、プログラム毎のパラメータの場合は第１ループ部に、エレメンタリ毎のパラメータの場合は第２ループ部に設定されるのが一般的である。以下の説明では、ＰＭＴにコンテンツＩＤを挿入する例を示す。

【０１４２】

ところで、上述のように、コンテンツＩＤをＥＣＭ以外に挿入する場合、コンテンツＩＤの不正な付け替えや改ざん等が行われてしまう危険性があるため、コンテンツとコンテンツＩＤとをセキュアにバインドする必要がある。そこで、コンテンツ取り込み装置１００におけるコンテンツ鍵情報暗号変換部１０３は、ＥＣＭを暗号変換する際に、コンテンツ

ＩＤを関連付けて暗号変換を行うことで、コンテンツとコンテンツＩＤとをセキュアにバインドする。具体的には、ネットワーク鍵とコンテンツＩＤのＸＯＲ（Ｅｘｃｌｕｓｉｖｅ　ＯＲ）をとったものや、ネットワーク鍵とコンテンツＩＤを結合したものを、ＥＣＭを再暗号化する暗号鍵として用いる方法や、コンテンツＩＤのハッシュをＳＨＡ－１等のハッシュアルゴリズムを用いて計算し、このハッシュ値をＥＣＭに挿入する方法や、ＥＣＭをコンテンツＩＤで暗号化した後、さらにネットワーク鍵で暗号化する方法などが挙げられる。以下の説明では、ネットワーク鍵とコンテンツＩＤのＸＯＲをとったものを、ＥＣＭを再暗号化する暗号鍵として用いる例を示す。

【０１４３】

以上のように構成されたコンテンツ利用システム３の動作を、図１８および図２０に示すフローチャートを用いて説明する。

図１８は、コンテンツ取り込み装置１００における、コンテンツ取り込み処理を示すフローチャートである。

【０１４４】

入力部１０１は、放送波からトランスポートストリームを受信する（ステップＳ１５０１）。

分離部１０２は、入力部１０１からトランスポートストリームを受け取り、ＴＳパケットのＰＩＤを参照して、コンテンツのＴＳパケットとＥＣＭのＴＳパケットを分離する（ステップＳ１５０２）。コンテンツおよびＥＣＭのＴＳパケットを示すＰＩＤは、ＰＭＴに記述されているので、これを参照して、ＴＳパケットの分離を行う。また、コンテンツＩＤを生成するため、ＳＩ情報を分離する。例えば、イベント情報が記述されたＥＩＴ（Ｅｖｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔａｂｌｅ）や現在時刻が記述されたＴＯＴ（Ｔｉｍｅ　Ｏｆｆｓｅｔ　Ｔａｂｌｅ）などである。

【０１４５】

コンテンツ鍵情報暗号変換部１０３は、ＥＣＭのＴＳパケットを受け取り、ＥＣＭセクションを再構成し、ワーク鍵を用いて暗号化されたＥＣＭを復号する（ステップＳ１５０３）。

【０１４６】

コンテンツ鍵情報暗号変換部１０３は、コンテンツＩＤ生成部１０４に対してコンテンツと共に配信されるデータ（ＥＩＴ、ＴＯＴの情報等）と共にコンテンツＩＤ生成要求を送り、コンテンツＩＤ生成部１０４はこれを受けて、コンテンツＩＤを生成する（ステップＳ１５０４）。ここで、コンテンツＩＤ生成部１０４は、例えばＥＩＴのｓｅｒｖｉｃｅ＿ｉｄと、ＴＯＴの現在時刻からコンテンツＩＤを生成する。この場合、コンテンツＩＤは時間単位で付与されることになる。さらに、このときにコンテンツ取り込み装置１００が内部で保持するユニークなＩＤを関連づけてコンテンツＩＤを生成すれば、グローバルユニークなコンテンツＩＤとすることができる。このように生成したコンテンツＩＤを、ＭＣＬを更新するために書き出しコンテンツリスト管理部１４０１に渡すと共に、コンテンツＩＤを記述したｃｏｎｔｅｎｔ＿ｉｄ＿ｄｅｓｃｒｉＰｔｏｒを生成するために多重化部１０５に渡す。また、コンテンツとコンテンツＩＤをセキュアにバインドするため、コンテンツＩＤをコンテンツ鍵情報暗号変換部１０３に渡す。

【０１４７】

書き出しコンテンツリスト管理部１４０１は、コンテンツＩＤ生成部１０４からコンテンツＩＤなどを受けると、書き出しコンテンツリスト蓄積部１４０２からＭＣＬを読み出し（ステップＳ１５０５）、コンテンツＩＤ生成部１０４から受け取ったコンテンツＩＤを登録する（ステップＳ１５０６）。なお、書き出しコンテンツリスト蓄積部１４０２にＭＣＬが無い場合は、ＭＣＬを生成して初期化を行う。

【０１４８】

ここで、ＭＣＬは図１９に示すように構成される。図１９に示したＭＣＬでは、現在までに蓄積メディアにコンテンツを書き出した回数として書き出し回数を記録すると共に、ある単位時間あたりの書き出し回数の上限（上限回数／単位）、および、あるコンテンツを

書き出してから、一定時間は当該コンテンツを書き出し不可とする制御を行うためのインターバルの時間（ペナルティ時間）、および、前回書き出しを行った時刻（前回書き出し時刻）とを記録するようになっている。例えば、コンテンツＩＤが「ＣＯＮＴＥＮＴ－ＩＤ－１１１１１」のコンテンツは、書き出しが１回行われていることを示しているが、単位時間あたりの書き出し回数の上限は、「２／Ｄａｙ」であるので、１日の間に２回は書き出すことができ、あと１回は蓄積メディアに書き出すことができることになる。また、ペナルティ時間については、「１ｈｏｕｒ」となっているため、前回書き出し時刻である「２２：２２：２２」から１時間の間（即ち、２３：２２：２２まで）は当該コンテンツを蓄積メディアに書き出すことが不可となるようなペナルティが課されるよう制御される。なお、本実施の形態では、単位時間あたりの書き出し回数の上限や、ペナルティ時間の設定を、コンテンツ毎に行うようにしたが、これらのパラメータをＭＣＬ毎に設定するようにし、ＭＣＬ毎に全コンテンツ共通の制約として用いても良い。

【０１４９】

また、書き出したコンテンツにマーキングを行う処理として、本実施の形態では、書き出し回数をインクリメントする（書き出していないコンテンツの場合は０のままである）ことにより、書き出したコンテンツと、一度も書き出していないコンテンツを区別するようにしている。

【０１５０】

書き出しコンテンツリスト管理部１４０１は、更新したＭＣＬを書き出しコンテンツリスト蓄積部１４０２に書き込む（ステップＳ１５０７）。

コンテンツ鍵情報暗号変換部１０３は、コンテンツＩＤ生成部１０４から受け取ったコンテンツＩＤとネットワーク鍵とを用いて、復号されたＥＣＭを再暗号化する（ステップＳ１５０８）。具体的には、コンテンツ鍵情報暗号変換部１０３は、内部で保持しているネットワークで予め共有された暗号鍵とコンテンツＩＤとのＸＯＲをとり、これを用いてＥＣＭを再暗号化する。さらに、このように再暗号化されたＥＣＭをＴＳパケット化して、多重化部１０５に渡す。

【０１５１】

多重化部１０５は、分離部１０２から受け取ったコンテンツのＴＳパケットと、コンテンツ鍵情報暗号変換部１０３から受け取った暗号変換後のＥＣＭのＴＳパケットとを多重化する。また、コンテンツＩＤ生成部１０４から受け取ったコンテンツＩＤからｃｏｎｔｅｎｔ＿ｉｄ＿ｄｅｓｃｒｉＰｔｏｒを生成し、ＰＭＴのディスクリプタ部に挿入する（ステップＳ１５０９）。

【０１５２】

このように、コンテンツ取り込み装置１００では、ＥＣＭの暗号が変換されることにより、ネットワークにバインドされたコンテンツが生成されると共に、コンテンツＩＤがＰＭＴに設定され、コンテンツと多重化される。また、ＭＣＬに取り込んだコンテンツのコンテンツＩＤが登録される。

【０１５３】

一方、図２０は、コンテンツ利用装置１１０ｂにおける、コンテンツ書き出し処理を示すフローチャートである。但し、コンテンツの書き出し可否をコンテンツ取り込み装置１００に問い合わせる処理を行うため、コンテンツ取り込み装置１００での処理も併せて図示している。

【０１５４】

分離部１１１において、コンテンツ取り込み装置１００から受け取ったトランスポートストリームから、コンテンツとＥＣＭを分離する。また、ＰＭＴを分離し、ＰＭＴのディスクリプタ部のｃｏｎｔｅｎｔ＿ｉｄ＿ｄｅｓｃｒｉＰｔｏｒからコンテンツＩＤを取得し、コンテンツ鍵情報復号部１１２に通知する（ステップＳ１７０１）。

【０１５５】

コンテンツ鍵情報復号部１１２は、分離部１１１から取得したコンテンツＩＤを、コンテンツＩＤ送信部１４０４に渡し、コンテンツＩＤ送信部１４０４は、コンテンツＩＤをコ

ンテンツ取り込み装置１００に送信する（ステップＳ１７０２）。

【０１５６】

コンテンツ取り込み装置１００のコンテンツＩＤ受信部１４０３は、コンテンツＩＤを受信し（ステップＳ１７０３）、受信したコンテンツＩＤを書き出しコンテンツリスト管理部１４０１に渡す。

【０１５７】

書き出しコンテンツリスト管理部１４０１は、書き出しコンテンツリスト蓄積部１４０２からＭＣＬを読み出す（ステップＳ１７０４）。

書き出しコンテンツリスト管理部１４０１は、コンテンツＩＤとＭＣＬとから、該当コンテンツの外部書き出し可否判定を行う（ステップＳ１７０５）。具体的には、ＭＣＬに登録されているコンテンツＩＤの単位時間あたりの上限回数や、ペナルティ時間を参照し、書き出しについて、制限内か否かを判定する処理を行う。

【０１５８】

ステップＳ１７０５において、ＹＥＳの場合、すなわち判定結果が書き出し可の場合、ＭＣＬの書き出し回数に１を加算してＭＣＬを更新し、書き出しコンテンツリスト蓄積部１４０２に蓄積する（ステップＳ１７０６）。また、判定結果をコンテンツＩＤ受信部１４０３に送信する。

【０１５９】

ステップＳ１７０５において、ＮＯの場合、すなわち判定結果が書き出し不可の場合、判定結果をコンテンツＩＤ受信部１４０３に送信する。

コンテンツ取り込み装置１００のコンテンツＩＤ受信部１４０３は、書き出しコンテンツリスト管理部１４０１から受け取った書き出し可否の判定結果を、コンテンツ利用装置１０６に送信する（ステップＳ１７０７）。

【０１６０】

コンテンツ利用装置１１０６のコンテンツＩＤ送信部１４０４は、コンテンツ利用装置１０６から書き出し可否の判定結果を受信し、判定結果をコンテンツ鍵情報復号部１１２に渡す（ステップＳ１７０８）。

【０１６１】

コンテンツ鍵情報復号部１１２は、書き出し可否の判定結果に従い、コンテンツの書き出し処理を行うかどうかを決定する（ステップＳ１７０９）。

ステップＳ１７０９において、ＹＥＳの場合、すなわち判定結果が書き出し可である場合、コンテンツ鍵情報復号部１１２は、分離部１１１から取得した再暗号化されたＥＣＭを取得し、ネットワーク鍵とコンテンツＩＤとのＸＯＲをとり、これを用いてＥＣＭを復号する（ステップＳ１７１０）。

【０１６２】

コンテンツ鍵情報復号部１１２は、ＥＣＭからコンテンツ鍵を取り出し、コンテンツ鍵をコンテンツ復号部１１６に渡すと共に、コンテンツ出力制御部１１５に対し、当該コンテンツをコンテンツ書き出し部１１９へ渡すように指示を行う（ステップＳ１７１１）。これにより、コンテンツ出力制御部１１５は、コンテンツ出力選択部１１７に対してコンテンツを書き出すように制御する。

【０１６３】

コンテンツ復号部１１６は、分離部１１１から取得したＴＳパケットを、コンテンツ鍵情報復号部１１２から取得したコンテンツ鍵で復号（デスクランブル）する（ステップＳ１７１２）。

【０１６４】

コンテンツ出力選択部１１７は、コンテンツ出力制御部１１５の制御に基づき、コンテンツを書き出すためのコンテンツ書き出し部１１９へコンテンツを受け渡す（ステップＳ１７１３）。

【０１６５】

コンテンツ書き出し部１１９は、コンテンツを蓄積メディアに書き出す（ステップＳ１７

１４）。具体的には、ＤＶＤ－ＲＡＭ、Ｄ－ＶＨＳ等の蓄積メディアに対応した形式で、コンテンツを暗号化したり、フォーマット変換したりして、蓄積メディアにコンテンツを書き出す。

【０１６６】

ステップＳ１７０９において、ＮＯの場合、すなわち判定結果が書き出し不可である場合、コンテンツ鍵情報復号部１１２は、コンテンツ書き出し処理を中止する。

【０１６７】

このように、本コンテンツ利用システム３では、ネットワークバインドされたコンテンツにコンテンツＩＤを付与し、同時にコンテンツ取り込み装置１００において管理するＭＣＬにコンテンツＩＤを登録し、コンテンツ利用装置１１０ｂは、コンテンツを書き出す際に、コンテンツ取り込み装置１００に書き出し可否を問い合わせ、コンテンツ取り込み装置１００がＭＣＬを用いて書き出し可否を判定することにより、無制限なコンテンツの書き出しに制限を課するようになっている。

【０１６８】

また、コンテンツ利用装置１１０ｂにおける、コンテンツ再生（表示）処理については、図２０と同様の処理の流れであるため、ここでは省略する。但し、ステップＳ１７０６の処理は常に行われないこと、および、コンテンツ出力制御部１１５からの指示により、ステップＳ１７１２でコンテンツ出力選択部１１７がコンテンツをコンテンツ表示部１１８に渡す処理を行い、コンテンツを再生する、というように修正が必要である。

【０１６９】

（実施の形態４）

以下、本発明の実施の形態４について、図面を用いて詳細に説明する。

図２１は、本発明の実施の形態４に係るコンテンツ利用システム４の構成を示すブロック図である。なお、本図において、図１６に示した実施の形態３のコンテンツ利用システム３と同様の構成要素については、図１６において既に説明しているので、図１６と同様の符号を付して以下の説明を省略する。

【０１７０】

図２１に示すコンテンツ利用システム４は、本発明の実施の形態３に挙げたコンテンツ利用システム３に対して、コンテンツ取り込み装置１００が、コンテンツＩＤ受信部１４０３に代えて、書き出しコンテンツリスト送信部１８０１を備え、コンテンツ利用装置１１０ｃが、コンテンツＩＤ送信部１４０４に代えて、書き出しコンテンツリスト受信部１８０２を備え、さらに、書き出しコンテンツリスト管理部１８０３と、書き出しコンテンツリスト蓄積部１８０４とを備え、コンテンツ取り込み装置１００がＭＣＬを管理し、コンテンツ利用装置１１０ｃは、コンテンツ取り込み装置１００からＭＣＬのコピーを受信し、受信したＭＣＬに基づいて、コンテンツの書き出しおよび表示を制御することを特徴とする。

【０１７１】

コンテンツ取り込み装置１００における書き出しコンテンツリスト送信部１８０１は、書き出しコンテンツリスト蓄積部１４０２に蓄積されているＭＣＬが更新されたとき、コンテンツ利用装置１１０ｃにＭＣＬを送信する。具体的には、コンテンツ取り込み装置１００が新たにコンテンツを取り込むことにより、ＭＣＬにコンテンツＩＤを登録する、あるいは、コンテンツ利用装置１１０ｃにおいて、コンテンツを書き出すことにより、コンテンツ利用装置１１０ｃから書き出したコンテンツのコンテンツＩＤを受信し、ＭＣＬの該当コンテンツＩＤに書き出した旨を表すマーキングを行ったときに、ＭＣＬを各コンテンツ利用装置１１０ｃに送信する。送信方法の一例としては、ブロードキャストする方法が挙げられる。

【０１７２】

コンテンツ利用装置１１０ｃにおける書き出しコンテンツリスト受信部１８０２は、コンテンツを書き出したとき、書き出したコンテンツのコンテンツＩＤをコンテンツ取り込み装置１００に送信し、コンテンツ取り込み装置１００において、ＭＣＬが更新されたとき

に、バージョンが更新された新しいＭＣＬを受信する処理を行う。

【０１７３】

コンテンツ利用装置１１０ｃにおける書き出しコンテンツリスト管理部１８０３は、書き出しコンテンツリスト蓄積部１８０４のＭＣＬを管理する。具体的には、コンテンツを書き出したとき、書き出したコンテンツのコンテンツＩＤを書き出しコンテンツリスト受信部１８０２に渡し、書き出しコンテンツリスト受信部１８０２が受信したＭＣＬを受け取り、書き出しコンテンツリスト蓄積部１８０４のＭＣＬを更新する、といった処理を行う。

【０１７４】

コンテンツ利用装置１１０ｃにおける書き出しコンテンツリスト蓄積部１８０４は、ＭＣＬを蓄積する部であり、ハードディスク等によって実現される。

以上のように構成されたコンテンツ利用システム４において、ＭＣＬをコンテンツ取り込み装置１００とコンテンツ利用装置１１０ｃとの間で同期する処理を、図２２および図２３に示すフローチャートを用いて説明する。なお、コンテンツ取り込み装置１００におけるコンテンツ取り込み時の処理は、本発明の実施の形態３において、図１８で示した動作と同様であるので、ここでは省略する。

【０１７５】

図２２は、コンテンツ利用装置１１０ｃにおける、コンテンツの書き出し処理を示すフローチャートである。

分離部１１１において、コンテンツ取り込み装置１００から受け取ったトランスポートストリームから、コンテンツとＥＣＭを分離する。また、ＰＭＴを分離し、ＰＭＴのディスクリプタ部のｃｏｎｔｅｎｔ＿ｉｄ＿ｄｅｓｃｒｉＰｔｏｒからコンテンツＩＤを取得し、コンテンツ鍵情報復号部１１２に通知する（ステップＳ１９０１）。

【０１７６】

コンテンツ鍵情報復号部１１２は、分離部１１１から取得したコンテンツＩＤを、書き出しコンテンツリスト管理部１８０３に渡すとともに、書き出しコンテンツリスト管理部１８０３は、書き出しコンテンツリスト蓄積部１８０４からＭＣＬを読み出す（ステップＳ１９０２）。このとき、書き出しコンテンツリスト蓄積部１８０４にＭＣＬが蓄積されていなければ、ＭＣＬを生成する。

【０１７７】

書き出しコンテンツリスト管理部１８０３は、コンテンツ鍵情報復号部１１２から受け取ったコンテンツＩＤがＭＣＬに存在するかどうかの検索を行う（ステップＳ１９０３）。

【０１７８】

ステップＳ１９０３において、ＮＯの場合、すなわちコンテンツＩＤがＭＣＬに存在しない場合は、当該コンテンツＩＤを書き出しコンテンツリスト管理部１８０３において、コンテンツ取り込み装置１００に送信するために、一時的に保持する（ステップＳ１９０４）。

【０１７９】

コンテンツ鍵情報復号部１１２は、分離部１１１からＥＣＭのＴＳパケットを受け取り、ＥＣＭセクションを再構成し、再暗号化されたＥＣＭを取得する。ネットワーク鍵とコンテンツＩＤとのＸＯＲをとり、ＥＣＭの暗号化部分を復号する（ステップＳ１９０５）。

【０１８０】

コンテンツ鍵情報復号部１１２は、ＥＣＭからコンテンツ鍵を取り出し、コンテンツ鍵をコンテンツ復号部１１６に渡すと共に、コンテンツ出力制御部１１５に対し、当該コンテンツをコンテンツ書き出し部１１９へ渡すように指示を行う（ステップＳ１９０６）。これにより、コンテンツ出力制御部１１５は、コンテンツ出力選択部１１７に対してコンテンツを書き出すように制御する。

【０１８１】

コンテンツ復号部１１６は、分離部１１１から取得したＴＳパケットを、コンテンツ鍵情報復号部１１２から取得したコンテンツ鍵で復号（デスクランブル）する（ステップＳ１

９０７）。
【０１８２】
コンテンツ出力選択部１１７は、コンテンツ出力制御部１１５の制御に基づき、コンテンツを書き出すためのコンテンツ書き出し部１１９へコンテンツを受け渡す（ステップＳ１９０８）。
【０１８３】
コンテンツ書き出し部１１９は、コンテンツを蓄積メディアに書き出す（ステップＳ１９０９）。具体的には、ＤＶＤ－ＲＡＭ、Ｄ－ＶＨＳ等の蓄積メディアに対応した形式で、コンテンツを暗号化したり、フォーマット変換したりして、蓄積メディアにコンテンツを書き出す。
【０１８４】
ステップＳ１９０３において、ＹＥＳの場合、すなわちコンテンツＩＤがＭＣＬに存在する場合は、ＭＣＬの該当コンテンツＩＤに関する情報を用いて、書き出し可否の確認を行う（ステップＳ１９１０）。具体的には、ＭＣＬには、コンテンツＩＤ毎に書き出し回数、単位時間あたりの書き出し回数の上限などが記録されるようになっているため、これらを参照して、書き出し可能かどうかの確認を行う。
【０１８５】
ステップＳ１９１０において、ＹＥＳの場合、すなわち書き出し可能と判定された場合は、当該コンテンツＩＤを書き出しコンテンツリスト管理部１８０３で一時的に保持する（ステップＳ１９０４）。ステップＳ１９０４以降の処理の詳細については前述の通りであるので、以降は省略する。
【０１８６】
ステップＳ１９１０において、ＮＯの場合、すなわち書き出し不可と判定された場合は、コンテンツ書き出し処理を中止する（ステップＳ１９１１）。
ここで、図２２におけるステップＳ１９０４で示したように、コンテンツ利用装置１１０ｃの書き出しコンテンツリスト管理部１８０３で一時的に保持したコンテンツＩＤを、コンテンツ取り込み装置１００に送信することにより、コンテンツ取り込み装置１００とコンテンツ利用装置１１０ｃとの間で、ＭＣＬの同期をとる処理を示すフローチャートを図２３に示す。なお、図２３では、複数のコンテンツ利用装置１１０ｃの内、コンテンツを書き出したコンテンツ利用装置１１０ｃをその代表として示しているが、その他のコンテンツ利用装置１１０ｃも新たなＭＣＬを受信し、同期する処理を行う。
【０１８７】
コンテンツ利用装置１１０ｃの書き出しコンテンツリスト管理部１８０３で保持されている、書き出したコンテンツのコンテンツＩＤは、書き出しコンテンツリスト受信部１８０２に渡され、ネットワークを通じてコンテンツ取り込み装置１００に送信される（ステップＳ２００１）。
【０１８８】
コンテンツ取り込み装置１００の書き出しコンテンツリスト送信部１８０１は、コンテンツＩＤを受信し（ステップＳ２００２）、書き出しコンテンツリスト管理部１４０１に渡す。
【０１８９】
書き出しコンテンツリスト管理部１４０１は、書き出しコンテンツリスト蓄積部１４０２のＭＣＬを読み出し（ステップＳ２００３）、受信したコンテンツＩＤをＭＣＬに追加あるいは更新し、書き出しコンテンツリスト蓄積部１４０２のＭＣＬを更新する（ステップＳ２００４）。このとき、ＭＣＬのバージョンを更新する。更新されたＭＣＬを書き出しコンテンツリスト送信部１８０１に渡す。
【０１９０】
書き出しコンテンツリスト送信部１８０１は、更新されたＭＣＬをコンテンツ利用装置１１０ｃに送信する（ステップＳ２００５）。例えば、全てのコンテンツ利用装置１１０ｃに対してブロードキャストする方法が挙げられる。

【０１９１】
コンテンツ利用装置１１０ｃの書き出しコンテンツリスト受信部１８０２は、更新されたＭＣＬを受信する（ステップＳ２００６）。受信したＭＣＬを書き出しコンテンツリスト管理部１８０３に渡す。
【０１９２】
書き出しコンテンツリスト管理部１８０３は、受け取ったＭＣＬのバージョンを参照し、保持しているＭＣＬのバージョンとの比較を行う（ステップＳ２００７）。
【０１９３】
ステップＳ２００７において、ＹＥＳの場合、すなわち受け取ったＭＣＬのバージョンが新である場合、書き出しコンテンツリスト蓄積部１８０４のＭＣＬを置換する（ステップＳ２００８）。なお、書き出しコンテンツリスト蓄積部１８０４にＭＣＬが蓄積されていなかった場合には、無条件で受け取ったＭＣＬを書き込む。
【０１９４】
ステップＳ２００７において、ＮＯの場合、すなわち受け取ったＭＣＬのバージョンが古い場合、受け取ったＭＣＬを破棄する。
このように、本コンテンツ利用システム４では、ネットワークバインドされたコンテンツにコンテンツＩＤを付与し、同時にコンテンツ取り込み装置１００において管理するＭＣＬにコンテンツＩＤを登録する。このＭＣＬを各コンテンツ利用装置１１０ｃに送信し、コンテンツを書き出す際には、各コンテンツ利用装置１１０ｃが保持するＭＣＬを用いて書き出し可否を判定することにより、無制限なコンテンツの書き出しに制限を課するようになっている。
【０１９５】
（実施の形態５）
以下、本発明の実施の形態５について、図面を用いて詳細に説明する。
図２４は、本発明の実施の形態５に係るコンテンツ利用システム５構成を示すブロック図である。なお、本図において、図３に示した実施の形態１のコンテンツ利用システム１と同様の構成要素については、図３において既に説明しているので、図３と同様の符号を付して以下の説明を省略する。
【０１９６】
本発明における実施の形態１～実施の形態４で挙げたコンテンツ利用システムでは、コンテンツ取り込み装置１００で取り込まれたコンテンツは、ネットワークで予め共有された暗号鍵のみを用いてコンテンツ鍵情報を再暗号化しているため、リアルタイムに利用することも可能であるし、ネットワーク上に接続されたハードディスク等の蓄積部に記録した後でコンテンツを利用することも可能であった。そのため、コンテンツを書き出す際にＭＣＬを用いて書き出しに制限を課するようにしていた。
【０１９７】
それに対し、本発明の実施の形態５で示すコンテンツ利用システム５では、コンテンツ取り込み装置１００において、コンテンツ取り込み時に、ある秘密情報を生成し、この秘密情報を作用させてコンテンツ鍵情報を再暗号化し、コンテンツ利用装置１１０ｄは、コンテンツを書き出す（再生する）際に、出力先を指定し、コンテンツ取り込み装置１００から秘密情報を取得することで、コンテンツを書き出す（再生する）ことができるようにしている。すなわち、コンテンツ利用装置１１０ｄからコンテンツ取り込み装置１００にコンテンツの出力先を指定し、出力先に従ってコンテンツをリアルタイムに蓄積メディアに書き出す、または再生するモードを設けるようにしたものである。ここで、コンテンツ取り込み装置１００において、コンテンツ利用装置１１０ｄから出力要求を受けた場合に、書き出し確認を行うことにより、コンテンツの書き出しに制限を課するようにすることができる。
【０１９８】
図２４に示すコンテンツ利用システム５は、コンテンツ取り込み装置１００が、入力部１０１と、分離部１０２と、コンテンツ鍵情報暗号変換部１０３と、多重化部１０５と、出

力要求処理部２１０１とを備え、コンテンツ利用装置１１０ｄが、分離部１１１と、コンテンツ鍵情報復号部１１２と、コンテンツ出力制御部１１５と、コンテンツ復号部１１６と、コンテンツ出力選択部１１７と、コンテンツ出力部としてコンテンツ表示部１１８およびコンテンツ書き出し部１１９と、出力要求部２１０２とを備え、コンテンツ取り込み装置１００のコンテンツ鍵情報暗号変換部１０３が、任意のタイミングで秘密情報を生成し、ネットワークで予め共有された暗号鍵（ネットワーク鍵）と、前記秘密情報とを用いてコンテンツ鍵情報を暗号化し、コンテンツ利用装置１１０ｄの出力要求部２１０２が、コンテンツの書き出しまたは再生を出力要求としてコンテンツ取り込み装置１００に出力要求を送信し、コンテンツ取り込み装置１００の出力要求処理部２１０１が、要求応答として前記秘密情報を送信し、コンテンツ利用装置１１０ｄの出力要求部２１０２が、前記要求応答から前記秘密情報を取得し、コンテンツ鍵情報復号部１１２は、前記ネットワーク鍵と前記秘密情報とを用いてコンテンツ鍵情報を復号し、コンテンツ鍵情報から取得したコンテンツ鍵を用いてコンテンツを復号し、コンテンツ出力選択部１１７は、出力先に応じたコンテンツの出力切り替えを行うことを特徴とする。

【０１９９】

コンテンツ取り込み装置１００におけるコンテンツ鍵情報暗号変換部１０３は、本発明の実施の形態１では、ネットワーク鍵を用いてＥＣＭを暗号変換していたが、本実施の形態では、コンテンツ取り込み時において、任意のタイミングで秘密情報を生成し、ネットワーク鍵と秘密情報を用いてＥＣＭを再暗号化するようにしている。秘密情報を生成するタイミングとして、例えば、番組（イベント）毎、コンテンツ毎に生成し、新たに生成した場合、以前の秘密情報は削除する。このように、秘密情報を有効としたい間だけ秘密情報を保持する方法により、出力するコンテンツを識別することができる。

【０２００】

コンテンツ取り込み装置１００における出力要求処理部２１０１は、コンテンツ利用装置１１０ｄからコンテンツの出力要求として、コンテンツの出力先と認証に用いるチャレンジを受信し、チャレンジからレスポンスを生成して、レスポンスと前記秘密情報をコンテンツ利用装置１１０ｄに要求応答として送信する。

【０２０１】

コンテンツ利用装置１１０ｄにおける出力要求部２１０２は、コンテンツ取り込み装置１００に対して、コンテンツを書き出すか、再生するかに応じた出力先と、認証に用いるチャレンジを送信する。出力要求の応答として、コンテンツ取り込み装置１００からレスポンスと前記秘密情報を受信し、レスポンスを認証する。認証に成功した場合にのみ、前記秘密情報をコンテンツ鍵情報復号部１１２に渡すように処理する。なお、チャレンジ・レスポンス認証については、本実施の形態では詳細に記述していないが、例えば、ＣＨＡＰ（Ｃｈａｌｌｅｎｇｅ Ｈａｎｄｓｈａｋｅ Ａｕｔｈｅｎｔｉａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）や、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ）において用いられるチャレンジ・レスポンスと同様の方法で認証処理が行われる。

【０２０２】

以上のように構成されたコンテンツ利用システム５の動作を、図２５および図２６に示すフローチャートを用いて説明する。

図２５は、コンテンツ取り込み装置１００における、コンテンツ取り込み時の処理を示すフローチャートである。

【０２０３】

入力部１０１は、放送波からトランスポートストリームを受信する（ステップＳ２２０１）。

分離部１０２は、入力部１０１からトランスポートストリームを受け取り、ＴＳパケットのＰＩＤを参照して、コンテンツのＴＳパケットとＥＣＭのＴＳパケットを分離する（ステップＳ２２０２）。また、コンテンツ鍵情報暗号変換部１０３がイベントを識別することを可能とするため、ＥＩＴのパケットを分離してコンテンツ鍵情報暗号変換部１０３に渡す。

【０２０４】
コンテンツ鍵情報暗号変換部１０３は、ＥＣＭのＴＳパケットを受け取り、ＥＣＭセクションを再構成し、ワーク鍵を用いて暗号化されたＥＣＭを復号する（ステップＳ２２０３）。また、受け取ったＥＩＴのＴＳパケットからＥＩＴを再構成し、イベント情報を取得する。
【０２０５】
コンテンツ鍵情報暗号変換部１０３は、イベント単位で秘密情報を生成する（ステップＳ２２０４）。具体的には、コンテンツ鍵情報暗号変換部１０３は、イベント毎に乱数で一定バイト長の秘密情報を生成する。
【０２０６】
コンテンツ鍵情報暗号変換部１０３は、生成した秘密情報とネットワーク鍵とを用いて、ＥＣＭを再暗号化する（ステップＳ２２０５）。具体的には、生成した秘密情報とある暗号アルゴリズム（例えばＡＥＳ等）を用いて、ＥＣＭのコンテンツ鍵の部分を暗号化する。さらに、ＥＣＭ全体をネットワーク鍵で暗号化する。この再暗号化されたＥＣＭをＴＳパケット化し、多重化部１０５に渡す。
【０２０７】
多重化部１０５は、分離部１０２から受け取ったコンテンツのＴＳパケットと、コンテンツ鍵情報暗号変換部１０３から受け取った暗号変換後のＥＣＭのＴＳパケットとを多重化する（ステップＳ２２０６）。
【０２０８】
このように、コンテンツ取り込み装置１００では、秘密情報を生成し、ＥＣＭをネットワーク鍵と秘密情報とを用いて暗号変換することにより、秘密情報を取得しない限りコンテンツの利用ができないように処理される。
【０２０９】
一方、図２６は、コンテンツ利用装置１１０ｄにおける、コンテンツ書き出し時の処理を示すフローチャートである。
コンテンツ利用装置１１０ｄの出力要求部２１０２は、リアルタイムの放送コンテンツを直接書き出す場合、コンテンツ取り込み装置１００と認証処理を行うためのチャレンジ（例えば乱数）を生成し、チャレンジデータとコンテンツの出力先（コンテンツ書き出し部１１９を指定する等）とを出力要求として、コンテンツ取り込み装置１００に送信する（ステップＳ２３０１）。
【０２１０】
コンテンツ取り込み装置１００の出力要求処理部２１０１は、コンテンツ利用装置１１０ｄからの出力要求として、チャレンジと出力先を受信する（ステップＳ２３０２）。
【０２１１】
出力要求処理部２１０１は、コンテンツの出力可否を判定する（ステップＳ２３０３）。具体的には、出力要求に含まれる出力先（書き出し先）を確認し、放送波に記述されるコピー制御情報やシステムで規定された書き出し先の制約と比較することにより、書き出し可能かどうかを決定する。また、あるコンテンツ利用装置１１０ｄとのチャレンジ・レスポンスを行った場合、ネットワーク上の他のコンテンツ利用装置１１０ｄからのチャレンジを受け付けない、あるいは、一定数のコンテンツ利用装置１１０ｄからのチャレンジまでは受け付けるようにすることにより、コンテンツの書き出しに制限を課するようにできる。
【０２１２】
ステップ２３０３において、ＹＥＳの場合、すなわち出力可と判定された場合には、チャレンジからレスポンスを生成し、要求応答として、レスポンスと秘密情報をメッセージに設定する（ステップＳ２３０４）。
【０２１３】
ステップ２３０３において、ＮＯの場合、すなわち出力不可と判定された場合には、その旨を示すエラーメッセージを生成し、要求応答としてメッセージに設定する。

【０２１４】
出力要求処理部２１０１は、要求応答をコンテンツ利用装置１１０ｄに送信する（ステップＳ２３０５）。
コンテンツ利用装置１１０ｄの出力要求部２１０２は、要求応答を受信し（ステップＳ２３０６）、レスポンスを認証する（ステップＳ２３０７）。
【０２１５】
ステップＳ２３０７において、ＹＥＳの場合、すなわち認証処理が成功した場合は、秘密情報を取得し、コンテンツ鍵情報復号部１１２に渡す（ステップＳ２３０８）。
【０２１６】
ステップＳ２３０７において、ＮＯの場合、すなわち認証処理が失敗した場合は、秘密情報を取得せず、コンテンツの書き出し処理を終了する。
コンテンツ鍵情報復号部１１２は、ネットワーク鍵を用いて再暗号化されたＥＣＭを復号し、さらに秘密情報を用いて、さらに暗号化されているコンテンツ鍵の部分を復号する（ステップＳ２３０９）。また、コンテンツ出力制御部１１５に対し、コンテンツの書き出し先、書き出し経路などを指示する。
【０２１７】
コンテンツ鍵情報復号部１１２は、復号されたコンテンツ鍵をコンテンツ復号部１１６に渡す（ステップＳ２３１０）。
コンテンツ復号部１１６は、分離部１１１から受け取った暗号化コンテンツを、コンテンツ鍵情報復号部１１２から受け取ったコンテンツ鍵で復号する（ステップＳ２３１１）。
【０２１８】
コンテンツ出力選択部１１７は、コンテンツ出力制御部１１５からのコンテンツ出力制御情報（コンテンツの書き出し先、書き出し経路など）に従い、コンテンツ書き出し部１１９にコンテンツを出力するよう選択する（ステップＳ２３１２）。
【０２１９】
コンテンツ書き出し部１１９は、コンテンツを蓄積メディアに出力する（ステップＳ２３１３）。
このように、本コンテンツ利用システム５では、リアルタイムに蓄積メディアに出力する（もしくは再生する）モードを設け、コンテンツ取り込み時に生成した秘密情報と、ネットワーク鍵とを用いてコンテンツ鍵情報を再暗号化することにより、秘密情報を取得できたコンテンツ利用装置１１０ｄでしかコンテンツを利用できないようにしている。すなわち、コンテンツ取り込み装置１００が、限られたコンテンツ利用装置１１０ｄにしか秘密情報を渡さないように制御すれば、ＭＣＬの蓄積や管理が不要であるため、構成をシンプルにすることができ、また、安全性が高いといった利点がある。例えば、複製が１回しか許されていないコンテンツ（コピー制御情報がＮＥＴＷＯＲＫ　ＣＯＰＹである等）の場合、コンテンツを取り込む際にコピー制御情報を参照することによって本モードを適用してコンテンツ鍵情報を暗号変換し、コンテンツ取り込み装置１００が唯１つのコンテンツ利用装置１１０ｄのみに秘密情報を渡すようにすると、ネットワークからは複製が１つのみ作れる、といったような制約を課することができる。
【０２２０】
なお、本実施の形態では、コンテンツ取り込み装置１００においてコンテンツ鍵情報を暗号化する際、コンテンツ取り込み時に生成した秘密情報と、ネットワーク上で予め共有された暗号鍵であるネットワーク鍵とを用いて暗号化を行なう場合の例を示したが、少なくともコンテンツ取り込み装置１００とコンテンツ利用装置１１０ｄとが共有する暗号鍵であれば、特にこれに限定されるものではない。
【０２２１】
（実施の形態６）
以下、本発明の実施の形態６について、図面を用いて詳細に説明する。
図２７は、本発明の実施の形態６に係るコンテンツ利用システム６構成を示すブロック図である。なお、本図において、図３に示した実施の形態１のコンテンツ利用システム１と

同様の構成要素については、図３において既に説明しているので、図３と同様の符号を付して以下の説明を省略する。

【０２２２】

図２７に示すコンテンツ利用システム６は、本発明の実施の形態１に挙げたコンテンツ利用システム１に対して、さらに、コンテンツを蓄積メディアに書き出す記録装置２４０１とで構成され、コンテンツ取り込み装置１００の構成は、本発明の実施の形態１でのコンテンツ取り込み装置１００と同様であるが、コンテンツ利用装置１１０ｅは、書き出しコンテンツリスト管理部１１３と、書き出しコンテンツリスト蓄積部１１４と、コンテンツ書き出し部１１９とが省かれており、記録装置２４０１が、コンテンツ書き出し部２４０２と、書き出しコンテンツリスト管理部２４０３と、書き出しコンテンツリスト蓄積部２４０４とを備え、記録装置２４０１がＭＣＬを管理し、コンテンツ利用装置１１０ｅから受信したコンテンツとコンテンツＩＤを蓄積メディアに書き出すとき、ＭＣＬを用いてコンテンツの書き出し可否を判定し、書き出し可否判定の結果に基づいて、コンテンツの書き出しを制御することを特徴とする。

【０２２３】

記録装置２４０１は、例えば、ＤＶＤ－ＲＡＭレコーダや、ＳＤカードリーダ／ライタなど、蓄積メディアへコンテンツを書き込むための装置が挙げられる。

コンテンツ書き出し部２４０２は、コンテンツを蓄積メディアに書き出すために必要な処理を行い、蓄積メディアにコンテンツを書き出す。

【０２２４】

書き出しコンテンツリスト蓄積部２４０４は、ＭＣＬを蓄積しておく部であり、ハードディスク等によって実現される。

書き出しコンテンツリスト管理部２４０３は、書き出しコンテンツリスト蓄積部２４０４に蓄積されるＭＣＬを管理する。具体的には、書き出しコンテンツリスト蓄積部２４０４からＭＣＬを読み出し、ＭＣＬを更新して書き出しコンテンツリスト蓄積部２４０４に書き込む、といったＭＣＬの読み書き処理や、蓄積メディアに書き出すコンテンツのコンテンツＩＤをコンテンツ書き出し部２４０２から受け取り、ＭＣＬを用いてコンテンツが蓄積メディアに書き出せるかどうかの判定を行う。

【０２２５】

以上のように構成された コンテンツ利用システム６の動作を、図２８に示すフローチャートを用いて説明する。

なお、コンテンツ取り込み装置１００におけるコンテンツ取り込み処理については、本発明の実施の形態１と同様であり、既に説明しているため、ここでは説明を省略する。

【０２２６】

図２８は、コンテンツ利用装置１１０ｅおよび記録装置２４０１における、コンテンツ書き出し処理を示すフローチャートである。

分離部１１１において、コンテンツ取り込み装置１００から受け取ったトランスポートストリームから、コンテンツとＥＣＭを分離する（ステップＳ２５０１）。

【０２２７】

コンテンツ鍵情報復号部１１２は、分離部１１１からＥＣＭのＴＳパケットを受け取り、ＥＣＭセクションを再構成し、再暗号化されたＥＣＭを取得する。ＥＣＭの暗号化部分を予め取得してあるネットワーク鍵で復号する（ステップＳ２５０２）。

【０２２８】

コンテンツ鍵情報復号部１１２は、ＥＣＭからコンテンツ鍵を取り出し、コンテンツ鍵をコンテンツ復号部１１６に渡す（ステップＳ２５０３）。また、コンテンツ出力制御部１１５に対し、コンテンツ出力選択部１１７でコンテンツを記録装置２４０１に出力するよう制御するため、書き込み先、書き込み経路などの情報を送信する。さらに、記録装置２４０１で、コンテンツ書き込み可否の判定に用いるコンテンツＩＤをＥＣＭから読み出し、コンテンツ出力制御部１１５に渡す。コンテンツ出力制御部１１５は、コンテンツＩＤと、書き込み先と、書き込み経路とをコンテンツ出力制御情報として、コンテンツ出力選

択部１１７に送信する。

【０２２９】

コンテンツ復号部１１６は、分離部１１１から取得したＴＳパケットを、コンテンツ鍵情報復号部１１２から取得したコンテンツ鍵で復号（デスクランブル）する（ステップＳ２５０４）。

【０２３０】

コンテンツ出力選択部１１７は、コンテンツ出力制御部１１５からのコンテンツ出力制御情報に基づき、記録装置２４０１へ出力を切り替え（ステップＳ２５０５）、コンテンツとコンテンツ出力制御情報を送信する（ステップＳ２５０６）。

【０２３１】

記録装置２４０１のコンテンツ書き出し部２４０２は、コンテンツ利用装置１１０ｅから、コンテンツとコンテンツ出力制御情報を受信する（ステップＳ２５０７）。受信したコンテンツ出力制御情報を、書き出しコンテンツリスト管理部２４０３に渡す。

【０２３２】

書き出しコンテンツリスト管理部２４０３は、書き出しコンテンツリスト蓄積部２４０４からＭＣＬを読み出し（ステップＳ２５０８）、書き出し可否判定を行う（ステップＳ２５０９）。ここでの書き出し可否判定は、本発明における実施の形態１で説明した方法と同様であるので、ここでは省略する。

【０２３３】

ステップＳ２５０９において、ＹＥＳの場合、すなわち書き出し可能と判定された場合は、ＭＣＬを更新し、書き出しコンテンツリスト蓄積部２４０４に蓄積する（ステップＳ２５１０）。また、コンテンツ書き込み処理の開始をコンテンツ書き出し部２４０２に指示する。

【０２３４】

コンテンツ書き出し部２４０２は、コンテンツを蓄積メディアに書き出す（ステップＳ２５１１）。

なお、ステップＳ２５０９において、ＮＯの場合、すなわち書き出し不可と判定された場合は、コンテンツ書き出し処理を終了する。

【０２３５】

このように、本コンテンツ利用システム６では、記録装置２４０１でＭＣＬを管理し、コンテンツを書き出す際にＭＣＬを用いて書き出し可否判定を行うことにより、レコーダ毎にコンテンツ書き出しの制限を課するようになっている。

【０２３６】

なお、コンテンツＩＤの生成方法について、コンテンツＩＤが単調増加または単調減少となるような生成部であれば、本発明における実施の形態１～実施の形態４、および、実施の形態６で示した方法に限定されるものではない。また、コンテンツＩＤがユニークな乱数値となるように生成しても良い。

【０２３７】

また、コンテンツＩＤの付与単位について、コンテンツのスクランブル単位でコンテンツＩＤを付与しても良い。あるいは、ユーザによる再生、録画等のボタン操作（ユーザのアクション）が行われる単位、具体的には、ユーザが録画開始を指示してから録画終了を指示するまで、あるいは、ユーザがあるチャネルを選択してから他のチャネルを選択するまで、などの単位でコンテンツＩＤを付与するようにしても良い。

【０２３８】

また、本発明における実施の形態１～実施の形態４、および、実施の形態６では、コンテンツ取り込み装置１００のコンテンツＩＤ生成部１０４においてコンテンツＩＤを生成する場合の例を示したが、コンテンツＩＤ生成部１０４を備えず、入力データ（例えば、ＥＩＴ等のコンテンツと共に配信されるデータ）に予め付与されている情報をコンテンツＩＤとして用いても良い。具体的には、デジタル放送の場合では、ＥＩＴに設定されているｓｅｒｖｉｃｅ＿ｉｄとｅｖｅｎｔ＿ｉｄとをそのままコンテンツＩＤとして利用したり

、送信側でコンテンツに付与したコンテンツＩＤが配信される場合は、このコンテンツＩＤを利用しても良い。

【０２３９】

また、本実施の形態では、コンテンツとコンテンツ鍵情報の対応付けを、多重化部１０５を用いて行う例を示したが、この手法はこの例に限られたものではなく、分離・多重を行わず、何らかの方法でコンテンツとコンテンツ鍵情報の対応付けをとっても良い。

【０２４０】

また、コンテンツ取り込み装置１００とコンテンツ利用装置１１０との間、あるいは、複数のコンテンツ利用装置１１０間、あるいは、コンテンツ利用装置１１０と記録装置２４０１との間で、ＭＣＬの確認を行うためにコンテンツＩＤを送受信したり、ＭＣＬの同期情報を送受信したり、コンテンツを送受信したり、コンテンツ出力制御情報を送受信したりするが、データの差し替え、改ざん防止のため、これらの通信の暗号化を行っても良い。

【０２４１】

また、少なくともコンテンツ取り込み装置１００におけるコンテンツ鍵情報暗号変換部１０８、コンテンツＩＤ生成部１０４や、コンテンツ利用装置１１０におけるコンテンツ鍵情報復号部１１２、書き出しコンテンツリスト管理部１１３、書き出しコンテンツリスト蓄積部１１４、コンテンツ出力制御部１１５は、セキュリティに係る処理を行う部であるため、セキュリティモジュールなどの耐タンパ化されたモジュールで実現しても良い。

【０２４２】

また、本発明における実施の形態１～実施の形態４では、コンテンツ利用装置１１０がコンテンツ表示部１１８とコンテンツ書き出し部１１９を備える場合の例を示したが、必ずしも両方を備える必要はなく、コンテンツ表示部１１８のみを備えるコンテンツ利用装置１１０や、コンテンツ書き出し部１１９のみを備えるコンテンツ利用装置１１０などであっても良い。この場合、コンテンツ出力制御部１１５あるいはコンテンツ出力選択部１１７の一方、または、両方を省略することもできる。

【０２４３】

さらに、本発明における実施の形態１～実施の形態６では、デジタル放送からＭＰＥＧ－２　ＳＹＳｔｅｍＳで多重化されたＭＰＥＧコンテンツを取り込む場合の例を示したが、本発明はこれに限られたものではなく、インターネット等の通信媒体やパッケージメディア等の記録媒体から任意のフォーマットのコンテンツを取り込む場合にも適用可能であることは言うまでもない。

【０２４４】

また、上記各実施の形態において、コンテンツ出力として、コンテンツをモニターに再生表示する表示部と、蓄積メディアに書き出す書き出し部とを有する例を示したが、これに限らず、ＩＥＥＥ１３９４等のデジタルバスに出力するようにしてもよい。このデジタルバスに出力する場合も、各実施形態における書き出し部と同様に出力可否を判定する構成とすればよい。

【０２４５】

さらに、上記各実施の形態におけるコンテンツ利用装置において、コンテンツ書き出し部は、ネットワークがコンテンツにバインドされていない状態での書き出しに加えて、バインドされた状態での書き出しをユーザの選択に応じて行う構成としてもよい。

【０２４６】

また、上記各実施の形態におけるＭＣＬのサイズが最大サイズに達し、コンテンツＩＤを追加できなくなった場合に、ＭＣＬから削除すべきコンテンツＩＤを乱数により決定して削除する構成としてもよい。

【０２４７】

さらに、上記各実施形態では、ＥＣＭ中に書き出し条件として最大書き出し回数、書き出し先、書き出し経路を設定可能であるが、書き出しの可否を示す情報をトランスポートストリーム中のＥＣＭ以外に設定する構成としてもよい。

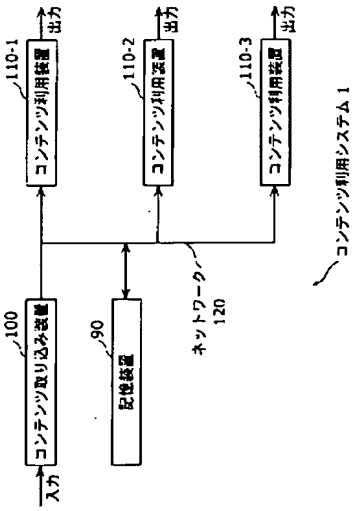
【０２４８】
また、上記各実施の形態におけるコンテンツ取り込み装置は、何れかのコンテンツ利用装置と物理的に一体であってもよい。
【０２４９】
（産業上の利用可能性）
本発明におけるコンテンツ利用システムは、ネットワークに接続されたコンテンツ取り込み装置と１以上のコンテンツ利用装置とからなる。コンテンツ取り込み装置は、コンテンツＩＤを発行するコンテンツＩＤ発行部と、ネットワーク上で予め共有されたネットワーク鍵でコンテンツ鍵情報を暗号変換するコンテンツ鍵情報暗号変換部とを備える。コンテンツ利用装置は、暗号変換されたコンテンツ鍵情報をネットワーク鍵で復号するコンテンツ鍵情報復号部と、蓄積メディアに書き出したコンテンツのコンテンツＩＤを記した書き出しコンテンツリスト（ＭＣＬ）を蓄積する書き出しコンテンツリスト蓄積部と、ＭＣＬに基づきコンテンツの書き出し可否判定を行う書き出しコンテンツリスト管理部とを備える。本発明は、上記の書き出し可否判定に従ってコンテンツの書き出しを行うコンテンツ利用システム、コンテンツ利用方法、コンテンツ利用装置、コンテンツ利用プログラムとして利用される。
【０２５０】
【発明の効果】
本発明のコンテンツ利用システムによれば、ネットワークにバインドされたコンテンツ毎に、コンテンツＩＤを付与して、コンテンツの書き出しテーブルによって管理するので、書き出し手段によって無制限に書き出しすることを抑制することができる。つまり、ネットワークにバインドされていない状態で書き出すことを制限することができる。例えば、家庭内のネットワークにバインドされたコンテンツを蓄積メディアに書き出したいという個人ユーザの要求を満たしながらも著作権を十分に保護することができるので、ユーザの私的利用と著作権者との間の相対立する利益をバランスよく満たすことができる。
【０２５１】
また、抑制手段は前記テーブルに当該コンテンツＩＤが既に存在していれば、前記書き出し手段に対して当該コンテンツの書き出しを抑制するので、書き出し手段による書き出しをコンテンツ毎に１回許可し、２回目以降を禁止することができる。
【０２５２】
また、抑制手段は、前記テーブルに当該コンテンツＩＤが存在し、かつ書き出し回数が予め定められた最大回数に達していれば、書き出し手段による書き出しを抑制するので、書き出し手段による書き出しをコンテンツ毎に最大回数の範囲内で許可し、それを超える場合は禁止することができる。最大回数は１つの値を予め定めておいてもよいし、コンテンツ毎に予め定めておいてもよいので、ユーザと著作権者との相対立する利益をより柔軟にバランスをとることができる。
【図面の簡単な説明】
【図１】本実施の形態に係るコンテンツ利用システムの全体の構成を示す図である。
【図２】本実施の形態に係るコンテンツ利用システムの全体の構成を示す図である。
【図３】実施の形態１に係るコンテンツ取り込み装置およびコンテンツ利用装置の構成を示す機能ブロック図である。
【図４】実施の形態１に係るＥＣＭセクションおよびＥＣＭの構成を示す図である。
【図５】実施の形態１に係る書き出しコンテンツリストの構成を示す図である。
【図６】実施の形態１に係るコンテンツ取り込み装置におけるコンテンツ取り込み処理を示すフローチャートである。
【図７】実施の形態１に係るコンテンツ利用装置におけるコンテンツ書き出し処理を示すフローチャートである。
【図８】実施の形態１に係るコンテンツ利用装置におけるコンテンツ再生処理を示すフローチャートである。
【図９】実施の形態１に係るコンテンツ利用装置におけるコンテンツ書き出し処理でのス

クランプルＩＤ生成、記録処理を示すフローチャートである。
【図１０】実施の形態１に係るコンテンツ利用装置における書き出し再開処理を示すフローチャートである。
【図１１】実施の形態２に係るコンテンツ取り込み装置およびコンテンツ利用装置の構成を示す機能ブロック図である。
【図１２】実施の形態２に係るコンテンツ利用装置間での書き出しコンテンツリスト同期処理を示すフローチャートである。
【図１３】実施の形態２に係る第１のコンテンツ利用装置での書き出しコンテンツリストの構成を示す図である。
【図１４】実施の形態２に係る第２のコンテンツ利用装置の書き出しコンテンツリストの構成を示す図である。
【図１５】実施の形態２に係る書き出し同期情報を示す図である。
【図１６】実施の形態３に係るコンテンツ取り込み装置およびコンテンツ利用装置の構成を示す機能ブロック図である。
【図１７】実施の形態３に係るＰＭＴおよびコンテンツＩＤを記述したｃｏｎｔｅｎｔ＿ｉｄ＿ｄｅｓｃｒｉＰｔｏｒの構成を示す図である。
【図１８】実施の形態３に係るコンテンツ取り込み装置におけるコンテンツ取り込み処理を示すフローチャートである。
【図１９】実施の形態３に係る書き出しコンテンツリストの構成を示す図である。
【図２０】実施の形態３に係るコンテンツ利用装置におけるコンテンツ書き出し処理を示すフローチャートである。
【図２１】実施の形態４に係るコンテンツ取り込み装置およびコンテンツ利用装置の構成を示す機能ブロック図である。
【図２２】実施の形態４に係るコンテンツ利用装置におけるコンテンツ書き出し処理を示すフローチャートである。
【図２３】実施の形態４に係るコンテンツ取り込み装置およびコンテンツ利用装置間での書き出しコンテンツリスト同期処理を示すフローチャートである。
【図２４】実施の形態５に係るコンテンツ取り込み装置およびコンテンツ利用装置の構成を示す機能ブロック図である。
【図２５】実施の形態５に係るコンテンツ取り込み装置におけるコンテンツ取り込み処理を示すフローチャートである。
【図２６】実施の形態５に係るコンテンツ利用装置におけるコンテンツ書き出し処理を示すフローチャートである。
【図２７】実施の形態６に係るコンテンツ取り込み装置およびコンテンツ利用装置および記録装置の構成を示す機能ブロック図である。
【図２８】実施の形態６に係るコンテンツ利用装置および記録装置におけるコンテンツ書き出し処理を示すフローチャートである。
【符号の説明】
１　コンテンツ利用システム
９０　記憶装置
１００　コンテンツ取り込み装置
１０１　入力部
１０２　分離部
１０３　コンテンツ鍵情報暗号変換部
１０４　コンテンツＩＤ生成部
１０５　多重化部
１１０　コンテンツ利用装置
１１１　分離部
１１２　コンテンツ鍵情報復号部
１１３　書き出しコンテンツリスト管理部

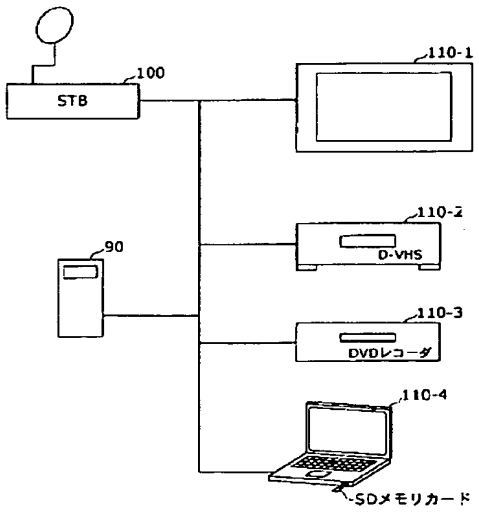
BEST AVAILABLE COPY

１１４　書き出しコンテンツリスト蓄積部
１１５　コンテンツ出力制御部
１１６　コンテンツ復号部
１１７　コンテンツ出力選択部
１１８　コンテンツ表示部
１１９　コンテンツ書き出し部
１２０　ネットワーク

【図１】

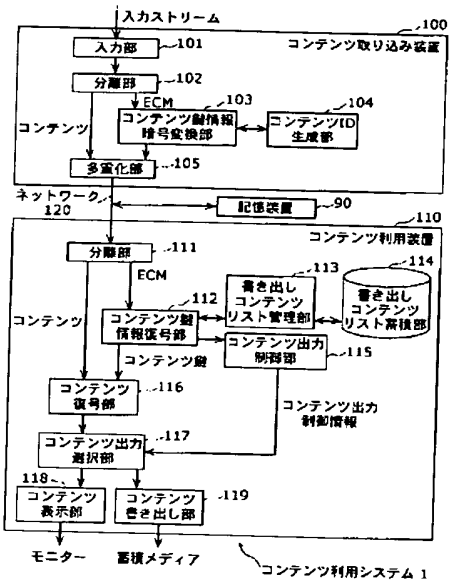


【図２】

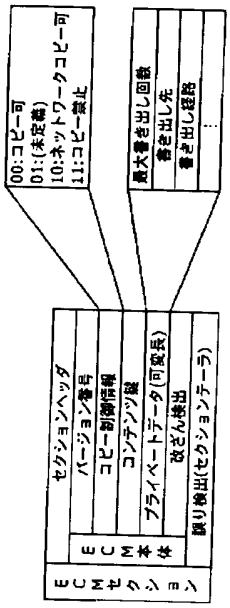


BEST AVAILABLE COP

【図３】



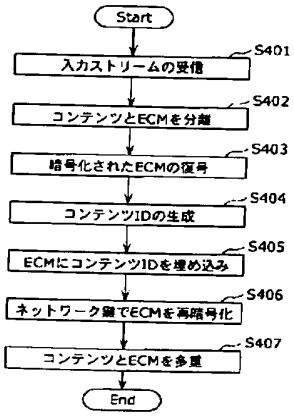
【図４】



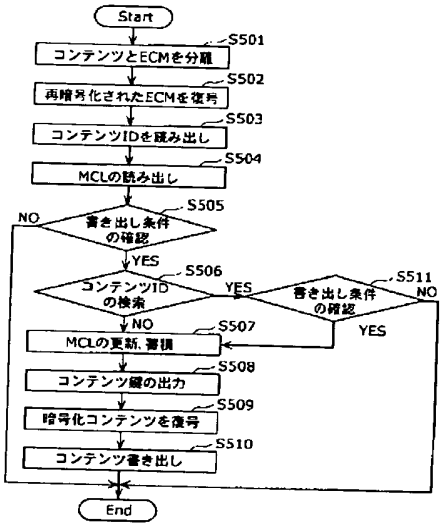
【図５】

コンテンツID	書き出し回数	書き出し先	書き出し経路
CONTENT-ID-11111	1	-	-
CONTENT-ID-22222	2	DVD-RAM	-
CONTENT-ID-88888	1	-	Digital(SD)
CONTENT-ID-55555	1	-	Analog
CONTENT-ID-77777	3	SDカード	-

【図６】

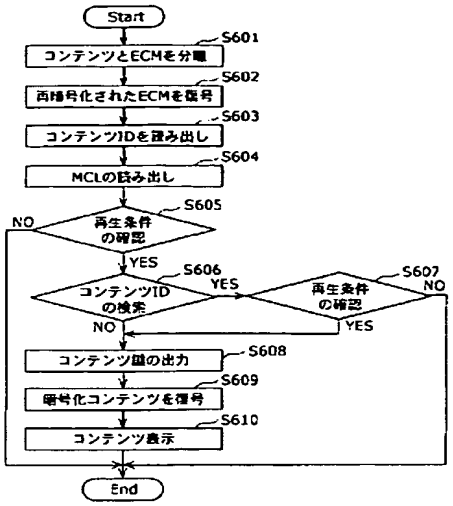


【図７】

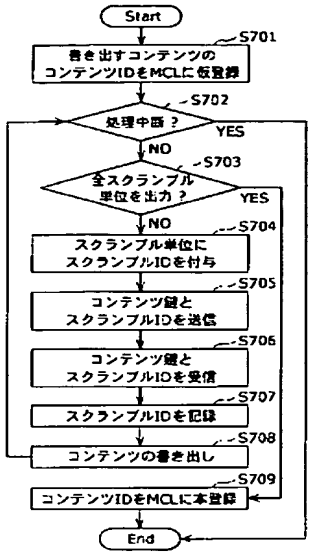


BEST AVAILABLE COPY

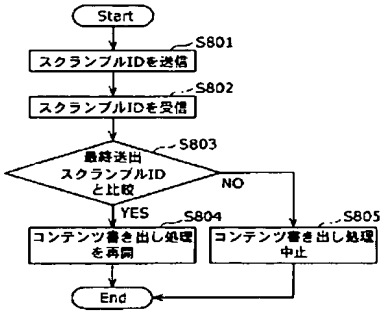
【図８】



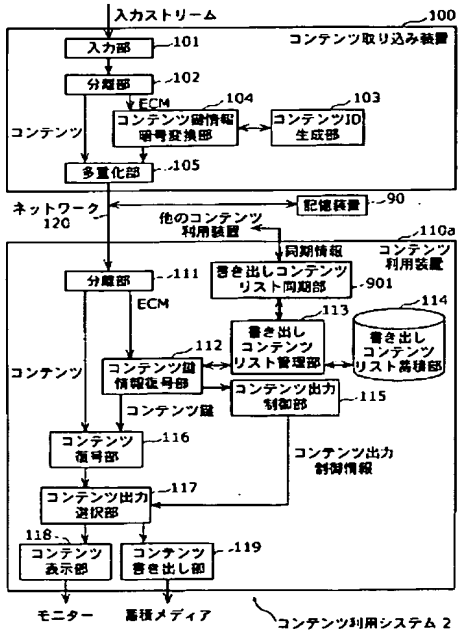
【図９】



【図１０】

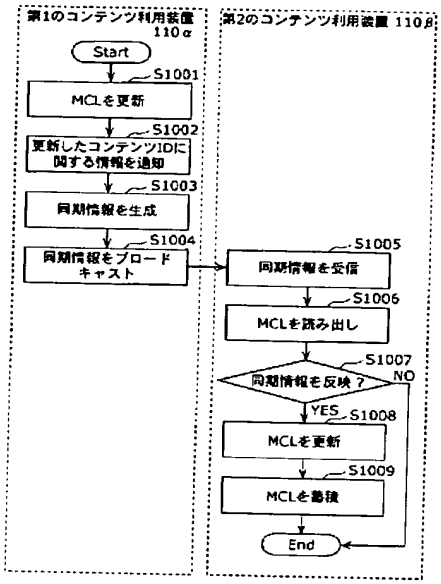


【図１１】



BEST AVAILABLE COPY

【図１２】



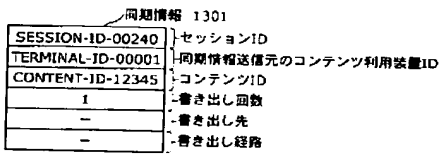
【図１３】

コンテンツID	書き出し回数/最大書き出し回数	書き出し先	書き出し経路
CONTENT-ID-11111	1/3	-	-
CONTENT-ID-22222	2/2	DVD-RAM	-
CONTENT-ID-88888	1/3	-	Digital(SD)
CONTENT-ID-55555	1/1	-	Analog
CONTENT-ID-12345	1/3	-	-

【図１４】

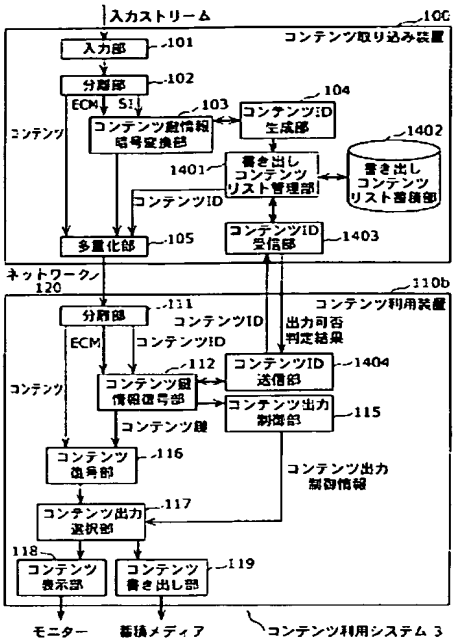
コンテンツID	書き出し回数/最大書き出し回数	書き出し先	書き出し経路
CONTENT-ID-11111	1/3	-	-
CONTENT-ID-22222	2/2	DVD-RAM	-
CONTENT-ID-88888	1/3	-	Digital(SD)
CONTENT-ID-55555	1/1	-	Analog

【図１５】

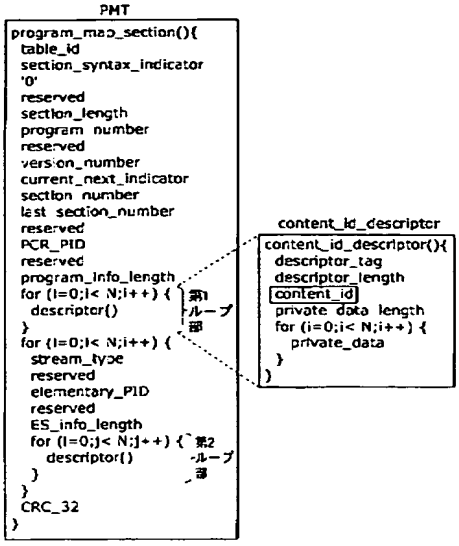


BEST AVAILABLE COPY

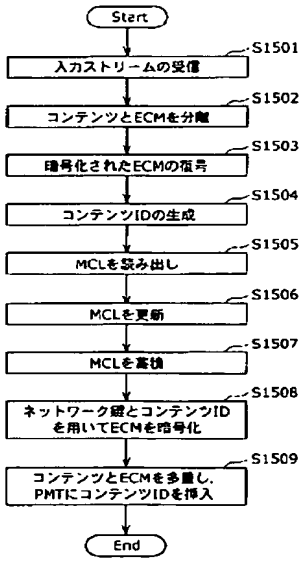
【図１６】



【図１７】



【図１８】

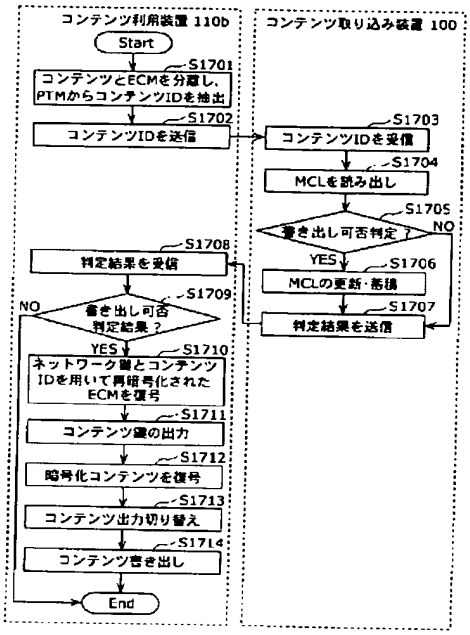


【図１９】

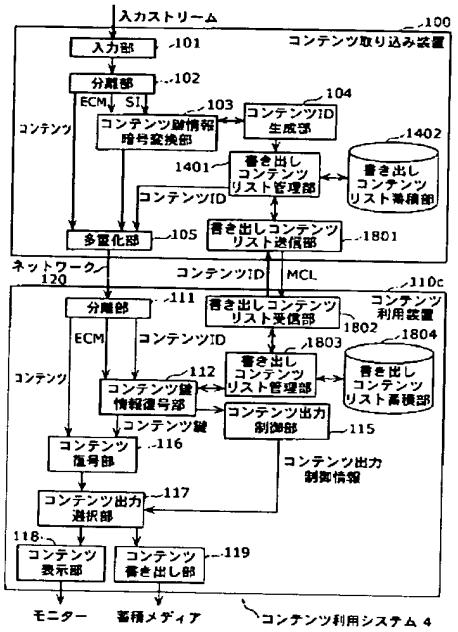
コンテンツID	書き出し回数	上限回数/単位	ペナルティ時間	前回書き出し時刻
CONTENT-ID-11111	1	2/Day	1hour	22:22:22
CONTENT-ID-22222	2	3/Hour	30min	12:05:12
CONTENT-ID-88888	0	3/Day	1hour	11:11:11
CONTENT-ID-55555	1	3/Day	1hour	1:02:03
CONTENT-ID-77777	0	1/Day	-	-

BEST AVAILABLE COPY

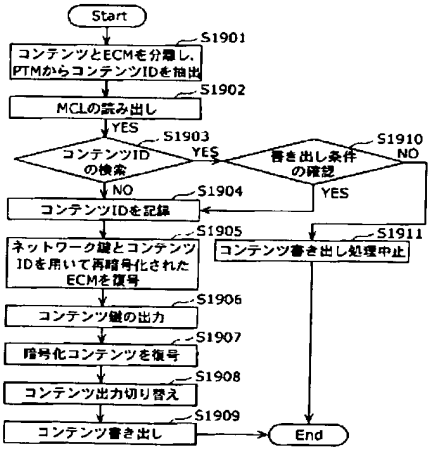
【図２０】



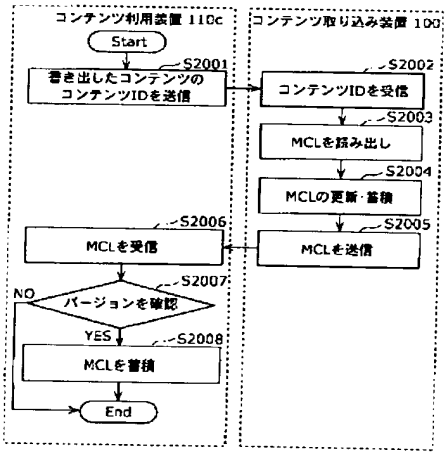
【図２１】



【図２２】

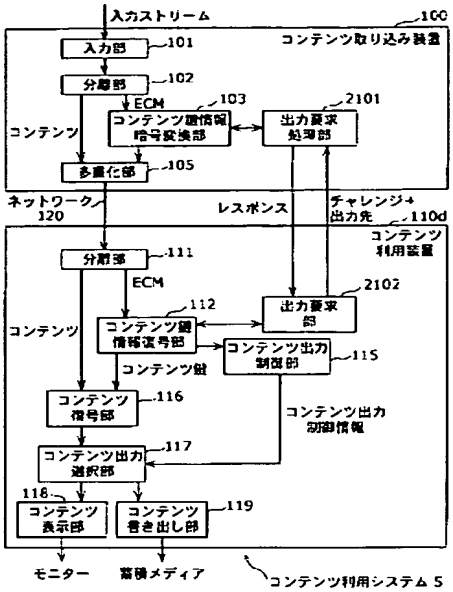


【図２３】

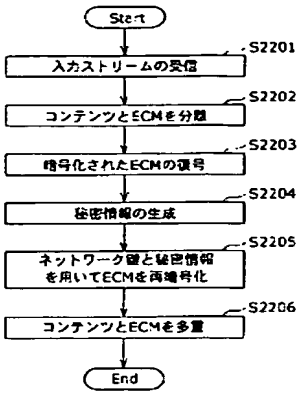


BEST AVAILABLE COPY

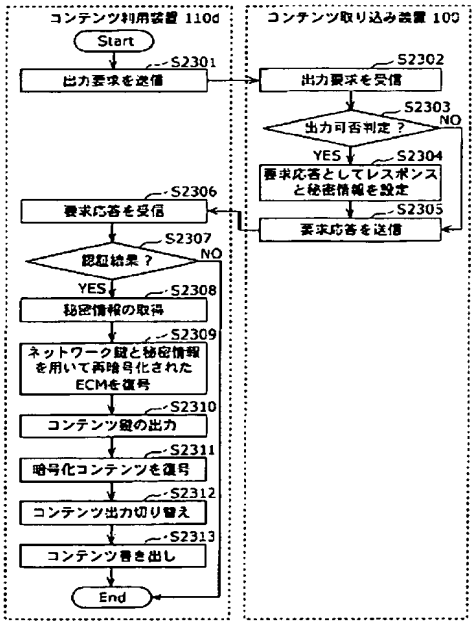
【図２４】



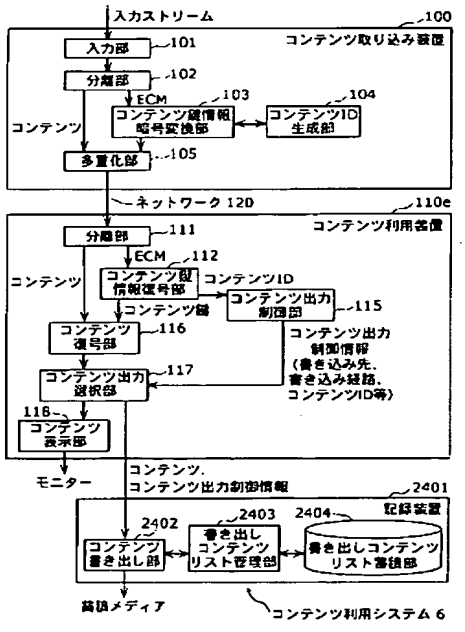
【図２５】



【図２６】

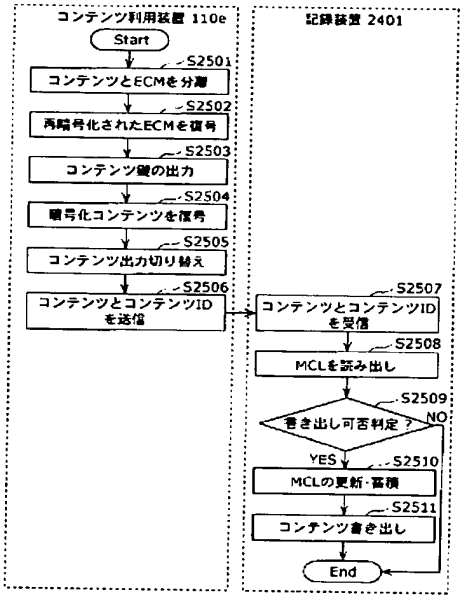


【図２７】



BEST AVAILABLE COPY

【図２８】



BEST AVAILABLE COPY

フロントページの続き

(51)Int.Cl.[7]	F I	テーマコード（参考）
	H04L 9/00 601E	

(72)発明者 井上 光啓
大阪府門真市大字門真１００６番地 松下電器産業株式会社内

Fターム(参考) 5B017 AA06 BA05 BB10 CA16
5J104 AA12 AA15 PA07 PA14

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)